6/25/87

ERRATA - REV. 1

The following modifications should be made to the LAVA 1.01 User's Manual.

Replace the last paragraph of Section 5.4, page 36 with the following.

> If you have a hard disk system, label and format as instructed below, two blank diskettes ANSWER and ANSWER(BACKUP). Then follow the instructions in the section "To Copy the ANSWER Diskette," omitting part 2 and copying COMMAND.COM from the C drive. (See the DOS manual for details on the use of the COPY command.)
>
> In a hard disk system with a single floppy disk drive, the terms "drive A" and "drive B" both refer to the same physical drive. It will be necessary to follow the instructions on the screen carefully, since both source and destination diskettes must use the same drive. Refer to the DOS manual for further details.

Add to Section 5.5, page 38 at the end of paragraph 6.

> Place write protect tabs on all the MASTER diskettes.

Delete from Section 5.7, pages 43 to 45, all references to working copies of DOS diskettes.

Add to Section 5.7, page 43 after paragraph 3.

> The CONFIG.SYS file will reside in the root directory of the hard disk.

Add to Section 6.1, page 69 before paragraph 1.

1. The system must be booted using the new CONFIG.SYS file. If you have turned the computer on since generating this file, that is sufficient. Otherwise, reboot at this time by pressing Ctrl-Alt-Del simultaneously. In a two floppy system the DOS system diskette must be in Drive A for the reboot.

LOS ALAMOS NATIONAL LABORATORY
3 9338 00214 4870

LAVA

for Computer Security

AN APPLICATION OF THE LOS ALAMOS VULNERABILITY ASSESSMENT METHODOLOGY

DOE Center for Computer Security

Release version 1.01
1987

Suzanne T. Smith - Los Alamos National Laboratory
Principal Investigator

and

Tracy Erkkila, Ray Leonard, David Martinez
Lynn Massagli, John Phillips, Mary Judy Roybal
Richard Tisinger
Lance Waller

LAVA Development Team

Copyright (c) 1983,1986 The Regents of the University of California

LAVA for Computer Security is an application of the LAVA methodology specific to computer and information security. LAVA/CS is a generic tool for identifying vulnerabilities in computer/information security safeguards systems. Version 1.01 does not perform a full risk assessment. However, the results from its analysis may provide valuable insights into security problems.

Copyright (C) 1983, 1986 The Regents of the University of California

Microsoft Quick BASIC Compiler Version 1.00
(C) Copyright Microsoft Corp. 1982, 1983, 1984, 1985

This software was produced by Los Alamos National Laboratory, an Affirmative Action/Equal Opportunity Employer. Los Alamos National Laboratory is operated by the University of California for the United States Department of Energy under contract W-7405-ENG-36. The U.S. Government is licensed to use, reproduce, and distribute this software. Permission is granted to the public to copy and use this software without charge, provided that this Notice and any statement of authorship are reproduced on all copies. Neither the Government nor the University makes any warranty, express or implied, or assumes any liability or responsibility for the use of this software.

This software is released through the DOE Center for Computer Security located at the Los Alamos National Laboratory, Los Alamos, New Mexico.

The development of this software was supported by funding from the following agencies:

United States Department of Energy
Office of Safeguards and Security

United States Department of Energy
Albuquerque Operations Office, IRED

United States Nuclear Regulatory Commission
Division of Automated Information Services
ADP Planning Staff

ACKNOWLEDGMENTS

DEVELOPMENT TEAM: Tracy Erkkila, Ray Leonard, Dave Martinez, Lynn Massagli, John Phillips, Mary Judy Roybal, Suzanne Smith, Dick Tisinger, Judy Lim, Lance Waller.

MANAGERIAL SUPPORT: Lara Baker, Arnie Hakkila, Jim Shipley, Jim Tape.

SECRETARIAL SUPPORT: Pat Anderson, Sharon Hurdle, Karen Knapp, Charlene McHale, Edith Williams.

PRESENTATION GRAPHICS: Sandy Bogenholm, Lucille Bonner, Lynne Williams, Kathy Jo Woodward.

TECHNICAL SUPPORT: Ralph Brickner, Susan Cupp, Josie Ford, Wendell Ford, John Hafer, Jan Hutson, Russell McFadden, Christi Stege.

OTHER SUPPORT: Alice Baker, Dan Baker, Buck Bassett, Al Bayse, Fran Berting, Arthur Boggs, Dave Brown, Blaine Burnham, Ron Butters, Mary Carlyon, Alton Coulter, Dave Diehl, Paul FitzGerald, Lou Grossman, Ralph Gutmacher, Duane Harder, Bill Hunteman, Irene Issac, Dave Jones, George Kapus, Stu Katzke, Jim Kirkpatrick, Bill Kirk, Vicki LaBarre, Jack Markin, Larry Martin, Ed Orner, Ted Orzechowski, Sylvan Pinsky, Don Richer, Don Roberts, Zella Ruthberg, Ron Smith, Dennie Steinauer, Mike Stevenson, Harold Sullivan, Marianne Swanson, Darrell Thomas, Gene Troy.

Contents

Part I

BACKGROUND

Chapter 1

INTRODUCTION

1.1 Organization of Manual

This user's manual is designed to help you learn about and use the Los Alamos Vulnerability Assessment tool for Computer Security (LAVA/CS). Once you are familiar with the LAVA/CS conventions and procedures, you may only need to refer to this manual for details.

BACKGROUND

CHAPTER 1. INTRODUCTION - Includes an overview of how the user's manual is structured and what you will need to run the LAVA/CS package.

CHAPTER 2. METHODOLOGY - Gives a brief description of the LAVA/CS methodology and the philosophy of the team approach to vulnerability assessments.

CHAPTER 3. THE VULNERABILITY REPORTS - Describes each of the reports generated by LAVA/CS and how to use them most meaningfully.

CHAPTER 4. THE DEMONSTRATION DISKETTE - Describes the demonstration diskette and includes instructions for installing and running the demonstration diskette.

TUTORIAL

CHAPTER 5. THE LAVA/CS TUTORIAL - Provides information regarding hardware, software, and operating system requirements. Instructs you on how to install the LAVA/CS software. Includes installation instructions for computer systems with both floppy disk drives and hard/fixed disks.

CHAPTER 6. ANSWERING THE QUESTIONNAIRE - Describes input conventions and definitions used in the questionnaire. Instructs you on how to answer the questionnaire.

CHAPTER 7. SCORING THE QUESTIONNAIRE - Describes how to obtain the vulnerability scores.

CHAPTER 8. PRINTING THE REPORT - Describes how to print the reports generated by LAVA/CS.

APPENDICES

Includes the regulatory basis for LAVA/CS, glossary of computer security terms, background information on the LAVA/CS methodology, a copy of the questionnaire, a bibliography, and user support information.

1.2 Hardware/Software Requirements

The LAVA/CS software has been written in dBaseIII. You do not need dBaseIII software to run LAVA; LAVA/CS Version 1.01 software is provided to you in compiled dBaseIII.

You will need the following hardware configuration at minimum:

1. IBM PC, IBM PC XT, or a computer that is 100% IBM compatible;
2. At least 512KB of memory;
3. One floppy disk drive AND one other storage medium (either another floppy disk drive or a fixed/hard disk);
4. IBM ProPrinter, Epson FX-80 printer or a 100% compatible printer.

You must provide a copy of MS-DOS or PC-DOS for "booting up" the computer before running LAVA/CS. The LAVA/CS package has been tested using PC DOS version 3.1, although it has been used successfully with versions 2.00 through 3.20.

1.3 What's in the 1.01 Package–A Parts List

In addition to the user's manual, the LAVA/CS Version 1.01 package contains the following diskettes:

INSTALLATION Diskette - The INSTALLATION Diskette is used to install LAVA/CS on a fixed or hard disk.

START Diskette - This disk is run first. It is used to define your facility and organization and determine the security level of the report.

ANSWER Diskette - The ANSWER Diskette is used as a storage diskette by LAVA/CS. It stores all answers and vulnerability scores and always resides in floppy disk drive A.

QUESTION Diskette - This diskette runs the interactive vulnerability assessment questionnaire.

SCORE Diskette - The SCORE Diskette calculates the vulnerability scores for your assessment.

REPORT Diskette - This diskette generates summary and detailed vulnerability reports.

DEMONSTRATION Diskette - The demonstration diskette gives you the feel of doing a vulnerability assessment by allowing you to answer a small subset of the questions. Please refer to the Background Section, Chapter 4 for additional information.

Please check immediately to see that your package contains all of the items listed above. If it does not, please refer to Appendix G for instructions.

Chapter 2

METHODOLOGY

2.1 What is LAVA ?

LAVA is an acronym for the Los Alamos Vulnerability Assessment methodology. It is a systematic method for assessing vulnerabilities in systems that can be characterized by a set of assets having some intrinsic value to the system, a set of threats against those assets, and a set of safeguards designed to protect the assets from the threats.

The assets, threats, and safeguards are specific to the application. The methodology delineates the steps that must be taken to model an application in terms of hierarchical disaggregation structures, the functional representations for safeguards-system objectives, the event trees for evaluating functional completeness, and the interactive questionnaires to elicit information about the safeguards system. The methodology gives both qualitative and quantitative insights into the vulnerabilities in the system of safeguards.

The LAVA methodology resulted from research efforts at the Los Alamos National Laboratory in Los Alamos, New Mexico. The complete methodology and the software implementation of the LAVA/CS algorithms, together with the development of application-specific data bases and questionnaires, permit the using organization to evaluate the completeness and adequacy of their organization's safeguards and security systems.

LAVA/CS Version 1.01 applies the vulnerability assessment segment of the LAVA methodology to a general computer- and information-security safeguards system. It assumes that the system is exposed to both natural and environmental hazards and to deliberate malevolent actions by either insiders or outsiders. The user in the process of answering the LAVA/CS questionnaire identifies missing safeguards in 34 areas ranging from password

management to personnel security and internal audit practices. Because of its modular structure, LAVA/CS allows the organization to evaluate the adequacy and completeness of individual safeguards areas and to reevaluate those same areas after missing safeguards have been initiated–without having to reanswer the entire questionnaire.

LAVA/CS considers specific safeguards protecting a generic set of assets (or targets) from a generic set of threats (or adversaries). There are four generic assets:

1. The FACILITY—the organization's environment.
2. The HARDWARE—all computer-related hardware.
3. The SOFTWARE—information in machine-readable form. Software includes data, output, programs, or system files stored on-line within the computer or on transportable media such as magnetic tapes, disks, or diskettes.
4. The DOCUMENTS and DISPLAYS—information in human-readable form. This includes manuals, data, computed results, program listings, output from a printer or plotter, reports on information stored within the computer system, displays on CRTs and terminals, information being processed by a printer or plotter, microfilm and microfiche, film output such as slides or movies, and hardcopy terminal output.

LAVA/CS considers two kinds of generic threats:

1. NATURAL and ENVIRONMENTAL HAZARDS—storms, fires, power outages and abnormalities, water damage, and accidental maintenance and housekeeping damage.
2. ON-SITE HUMAN THREATS — both intentional and accidental acts requiring the perpetrator to be on the premises at the facility.

In short, LAVA/CS is an automated, simple to use, easy to understand (even for those unversed in risk analysis), interactive, and portable vulnerability assessment package. It produces general summary reports for management personnel, as well as detailed reports for use by operations staff. The vulnerability scores are given as both quantitative values and linguistic descriptors and are combined with impact measures to provide useful measures of risk.

2.2 The Team Approach

The LAVA philosophy is based upon the team approach. This concept is vital to arriving at results that depict the actual safeguards in place. There are two parts to the assessment team:

1. A core team (a minimum of five people is suggested) whose members are present throughout the entire interactive assessment period, and
2. A transient team whose members participate during the periods in which their expertise is required.

Both teams should be present for the preliminary session at the start of the formal assessment.

The purpose of the team approach is to ferret out real information–the kind of information that is often taken for granted but, when the situation is examined more closely, turns out to be quite different from what was assumed originally. The entire assessment team, supplemented by a few experts who might be called in briefly, should be able to reach a consensus reflecting the true situation.

LAVA requires the team members to have specialized knowledge about the following aspects of the facility and its assets:

1. physical security
2. technical security
3. building engineering
4. heating, ventilating and air conditioning
5. fire protection
6. building maintenance and housekeeping
7. computer operations
8. systems programming practices
9. applications programming practices
10. computer room security practices
11. budget and accounting

12. personnel
13. long-range planning
14. upper-level management
15. electrical systems
16. local telephone system
17. plumbing
18. internal audit
19. external audit
20. payroll

The quality of the assessment depends upon the experiences of the team members—the broader the spectrum of backgrounds and expertise, the more thorough the assessment will be.

REACHING A CONSENSUS BEFORE ENTERING AN ANSWER IN THE QUESTIONNAIRE IS VITALLY IMPORTANT. Because the team members have different backgrounds, they may take different points of view and may approach the same question from many different ways. The discussions held while trying to reach the consensus can be enlightening to everyone present.

One of the side benefits an organization receives by using LAVA is that simply going through the questionnaire in the team environment is a good exercise in consciousness-raising. Another benefit is that the team interactions open the communications channels within the organization by bringing together individuals who would not ordinarily have much contact with one another.

2.3 Items You May Need for Reference

The following materials may be helpful to facilitate answering questions during the interactive assessment.

1. A scale floor plan of both the computer room and the area that shows the location of all
   (a) doors, windows, attached offices, user work areas;

(b) supply rooms, media storage rooms, communications closets, and specific pieces of the system hardware;

(c) ceiling and under-floor smoke detection and fire detection devices;

(d) automatic fire protection devices;

(e) manually operated alarm switches, fire extinguishers, and emergency lights;

(f) water detection devices;

(g) monitors, alarms, motion detectors, closed-circuit television cameras, and recording devices; and

(h) guard stations and personnel identification devices.

2. A copy of the Data Center Emergency Response Plan (DCERP).

3. A list of all pieces of machine-readable information stored in the computer system that are considered sensitive, classified, or otherwise merit protection; a list of the locations of these pieces of information.

4. A list of pieces of human-readable information that are considered to be sensitive, classified, or otherwise merit protection; a list of the locations of these pieces of information.

5. A list of computer system components.

6. A list of all other hardware items necessary for computer operation.

   Such items may include air-conditioning units and back-up power supplies. Product descriptions of the listed hardware may prove useful.

7. System management documents and daily operations reference documents.

2.4 Performing An Assessment with LAVA/CS

Before you begin your vulnerability assessment, be sure you have read Section 2.2 (The Team Approach) and understand the importance of performing an assessment using the team concept.

The first step in performing a vulnerability assessment using LAVA/CS is to appoint or select a Lead Assessor. The Lead Assessor has several responsibilities in addition to the responsibilities of an assessment team member. The responsibilities of the Lead Assessor include:

1. determining the time period for the assessment, and selecting a core team that can be present throughout the entire assessment period;

2. selecting members of the transient team, and alerting other experts who may be called in to resolve issues that cannot be decided upon during group discussion;

3. distributing in advance a copy of the LAVA/CS questionnaire to each member of the entire assessment team for their review. This is an important task, and the Lead Assessor should urge the team members to familiarize themselves with the questionnaire and to undertake any preliminary research that might be indicated;

4. making arrangements to reserve a conference room for the entire assessment period. The interactive part of the assessment will take place in this conference room;

5. making arrangements for the entire assessment team to tour the computer center as a group on the first day of the assessment. The Lead Assessor should make arrangements for computer center personnel to be on hand to answer any questions that may arise during the walk-through;

6. scheduling approximate interaction times for the transient team;

7. understanding the LAVA/CS vulnerability assessment process in enough depth to be able to explain the assessment process to other team members, management, or curious onlookers;

8. being present throughout the entire assessment period, and to guide gently any discussion that appears to be at a stalemate. The Lead Assessor should be ready to call in an expert if the occasion warrants;

9. KEEPING THE TEAM FROM ENTERING AN ANSWER UNTIL THEY HAVE REACHED A CONSENSUS; and

10. executing the scoring, printing the vulnerability report and distributing copies of the report to the assessment team. The Lead Assessor should lead the team in discussion after they have reviewed the report.

A vulnerability assessment performed with LAVA/CS takes a few days of preparation, two to four days of team discussions and interactions while answering the questionnaire, and a day to execute the scoring, print the

report, distribute copies to team members, and discuss the results of the assessment.

2.5 Terminology, Definitions and Conventions

2.5.1 Terminology

The term, Organization, used in LAVA/CS refers to the parent organization for the site performing the vulnerability assessment. Organization does not refer to the suborganization responsible for computer operations.

A sample organization is the Los Alamos National Laboratory. This organization's grounds cover several hundred square miles, and it has many suborganizations (or divisions). Each of the divisions is subdivided into groups. For example, the Computer Division that contains eight groups, one of which is responsible for the operation of the Central Computing Facility. However, other divisions and groups within the Laboratory have their own computer(s), all of which must have independent vulnerability assessments performed. These divisions or groups, although they are within a common geographical area, may be located in separately controlled areas and may have several buildings within a common fence. They may be separated from other fenced areas by considerable distances. Nevertheless, the policies and procedures of the Los Alamos National Laboratory affect all divisions and groups. To reiterate the important concept, the parent organization in this example is the Los Alamos National Laboratory.

The term, adversary, is occasionally referred to in the questionnaire. We define adversary to mean a deliberate malefactor, either an insider (such as an employee, vendor, or contractor) or an outsider. Do not be fooled into thinking that because an employee has a clearance, his intentions are honorable. More than two-thirds of all computer crime, damage, and misuse is perpetrated by someone on the inside.

2.5.2 Definitions

Using the following definitions for "Facility" (an organization's environment), "Perimeter Zone," "Building," "Area," "Computer Room(s)," and "Computer System," the assessment team should reach a consensus about the boundaries of these terms relative to the facility, procedures, and physical plant on which the vulnerability assessment is being performed. We recommend that the team make a sketch of the facility that clearly indicates

these boundaries. The sketch should be displayed prominently throughout the assessment period for reference and included in the final report for future reference.

We use the following definitions in LAVA/CS:

Facility - (Organization's environment) is the physical and procedural environment of the parent organization and may include one or more information processing center(s). It may include several buildings, their surrounding grounds (if any), the equipment necessary for operations, and the procedures established by the organization for conducting both normal business and emergency situations. It is not restricted only to buildings in which the actual information processing takes place. It also includes those buildings and surrounding grounds in which information in any form exists about, processed by, or related to the information-processing center and its parent organization.

The facility includes the policies and procedures established by the organization, support hardware for the computer center (such as power, heating, air conditioning), security practices, personnel, and other items relating to the physical surroundings.

Perimeter Zone - The organization's grounds and buildings may be delimited by a perimeter zone that may or may not be fenced. In the case of an organization that has extensive land and several sites (fenced or unfenced), each of whose perimeter zone access is controlled separately by site, then this definition should include ONLY the area logically associated with the individual site for which the assessment is being performed.

Building - The building is the specific structure(s) that houses the computer installation being assessed. It includes all buildings housing the information-related activities described in the following definitions of area, computer room, and computer system.

Area - The area comprises the locations where both computer-related activities take place and where information considered by the organization to be worthy of protection is held, used, processed or stored. The area need not be contiguous to the computer room(s). It may contain user work areas, general office space, laboratories, input or program keying areas, storage areas, places for submitting input to the computer(s) or

to input/program keying personnel, places to retrieve and peruse output, remote terminals, document libraries, microfilm/microfiche processing equipment and/or readers, and related items.

Computer Room - The computer room is a partitioned space housing the data-processing and related equipment. This may include media vaults, telecommunications closets, office space for system support personnel, maintenance workshops and limited storage space for related supplies. In the LAVA/CS questionnaire the tape library is considered to be part of the computer room.

Computer System - The computer system encompasses both the computer-related machinery and the storage media upon which information (programs, data, results) is stored in non- human-readable form.

2.5.3 Conventions

In computer systems with dual disk drives, LAVA/CS consistently refers to the disk drive on the left (or top) as drive A and to the disk drive on the right (or bottom) as drive B. In computer systems with a hard/fixed drive, we refer to the default drive as drive C.

The symbols < > are used to indicate the name for a specific key on the keyboard. For example, `<Ctrl C>` means to press the C key while holding down the `Ctrl` key.

The symbol `<CR>` means carriage return; we use it synonymously with the keys "Enter" and "Return". The `<CR>` command is used to enter your input into the computer. You must follow all input from the keyboard with a carriage return. When we refer to `<CR>` in the text of this manual, we are asking you to press the carriage return `<CR>` key on your keyboard. On the IBM PC XT keyboard, the carriage return is the key with the downward hooked arrow.

During the course of answering the questionnaire and at other times during the assessment, LAVA/CS will ask for your response to a variety of questions. Most of these questions require a "Yes" or "No" response. LAVA/CS will accept Y, y, N, or n as input to the "Yes/No" questions.

Chapter 3

THE VULNERABILITY REPORTS

3.1 How to Use and Interpret the Results of LAVA/CS

LAVA/CS can be used to assess the vulnerabilities of safeguards systems for computer systems. External requirements, as well as good management practices, require that management routinely review their susceptibility to loss or unauthorized use of resources. LAVA/CS provides an easy-to-use tool for assessing potential vulnerabilities while having a minimal impact upon the operations of the computer facility. The same software package can be used periodically to determine if changes in the operations or changes within the facility have increased or decreased the vulnerability of the computer system.

The Report Generator produces summary tables and specific plots of the vulnerabilities of the individual safeguards functions and subfunctions. Five sections are generated

1. Ordered Ranking of Vulnerabilities,
2. Summary of Vulnerabilities of Specific Threats,
3. Scatter Diagrams of Safeguards Functions,
4. Bar Charts of Individual Safeguards Functions, and
5. Detailed Plots of Event Trees and Listings of Vulnerabilities.

The first four pages of the report (pages i through iv) contain administrative information about the facility and the individuals who performed the vulnerability assessment. The information in each of the five sections of the report will be summarized in the following pages.

3.2 Ordered Ranking of Vulnerabilities

This summary ranks the vulnerabilities of the individual safeguards subfunctions and their associated vulnerability fractions. A low vulnerability value is better than a high one. A value of 1.00 implies that the safeguards function does not exist—a maximum vulnerability. However, one must be careful when interpreting these values because a specific facility may not have any control over the listed safeguards functions, and therefore a maximum vulnerability of 1.00 may be inherent in the system. The absolute values are not as important as are the relative values that can be used to identify areas of high vulnerability. A value of 0.8 should not be interpreted as being significantly different from a value of 0.7.

********** UNCLASSIFIED SENSITIVE **********

LAVA/CS VULNERABILITY REPORT * page 2 *

ORDERED RANKING OF VULNERABILITIES
(Note: A low score is better than a high score)

VULNERABILITY	SCORE
HARDWARE REACHABILITY CONTROL; PERIMETER	1.00
DATA, DISPLAY & DOC. REACHABILITY CONTROL; ROOM	1.00
DATA, DISPLAY & DOC. REACHABILITY CONTROL; AREA	1.00
WATER DAMAGE CONTROL; DETECTION	1.00
ORGANIZATION REACHABILITY CONTROL; ROOM	1.00
ORGANIZATION REACHABILITY CONTROL; PERIMETER	1.00
SOFTWARE REACHABILITY CONTROL; PERIMETER	1.00
DATA, DISPLAY & DOC. REACHABILITY CONTROL; PERIMETER	1.00
SOFTWARE REACHABILITY CONTROL; AREA	1.00
HARDWARE REACHABILITY CONTROL; AREA	1.00
HVAC DAMAGE CONTROL; DETECTION	1.00
SOFTWARE REACHABILITY CONTROL; ROOM	1.00
HARDWARE REACHABILITY CONTROL; ROOM	1.00
ORGANIZATION REACHABILITY CONTROL; AREA	1.00
HARDWARE INVENTORY & BACKUP CONTROL; BACKUP CONTROL	0.86
FIRE DAMAGE CONTROL; DETECTION AND ALARMS	0.82
HVAC DAMAGE CONTROL; MITIGATION	0.55
FIRE DAMAGE CONTROL; PREVENTION	0.52
FIRE DAMAGE CONTROL; MITIGATION	0.51
SOFTWARE APPLICATION CONTROL; DEV. & PROG. CHNG.	0.42
SOFTWARE APPLICATION CONTROL; ERR. PREV. & DETECTION	0.42
SOFTWARE APPLICATION CONTROL; SOFTWARE USE	0.34
WATER DAMAGE CONTROL; MITIGATION	0.33
DATA, DISPLAY & DOC. ERROR CORR. & BACKUP; BACKUP CONTROL	0.33
ORGANIZATION PERSONNEL MEASURES; EMERG. SERV. PERS. MONT.	0.32
SOFTWARE AUDIT CONTROL; INTERNAL AUDIT	0.29
ORGANIZATION ACCESS CONTROL; VEND., SERV., VISITOR	0.29
HVAC DAMAGE CONTROL; PREVENTION	0.27
MAJOR HAZARD DAMAGE CONTROL; EXPOSURE	0.27
ORGANIZATION PERSONNEL MEASURES; EMP. STAT. MONITORING	0.26
FIRE DAMAGE CONTROL; ADMINISTRATION	0.25
WATER DAMAGE CONTROL; PREVENTION	0.24
SOFTWARE APPLICATION CONTROL; CORRECTION & BACKUP	0.24
HARDWARE REACHABILITY CONTROL; BUILDING	0.23
ORGANIZATION REACHABILITY CONTROL; BUILDING	0.23
DATA, DISPLAY & DOC. REACHABILITY CONTROL; BUILDING	0.23
SOFTWARE REACHABILITY CONTROL; BUILDING	0.23
MAJOR HAZARD DAMAGE CONTROL; RESISTANCE	0.22
HARDWARE INVENTORY & BACKUP CONTROL; INVEN/AUDIT CONTROL	0.21
POWER OUTAGE DAMAGE CONTROL; MITIGATION	0.21
ORGANIZATION ACCESS CONTROL; AUTHORIZATION	0.21
EMERGENCY SERVICE CONTROL; EMERGENCY RESPONSE	0.20

********** UNCLASSIFIED SENSITIVE **********

Ordered Ranking of Vulnerabilities

3.3 Summary of Vulnerabilities of Specific Threats

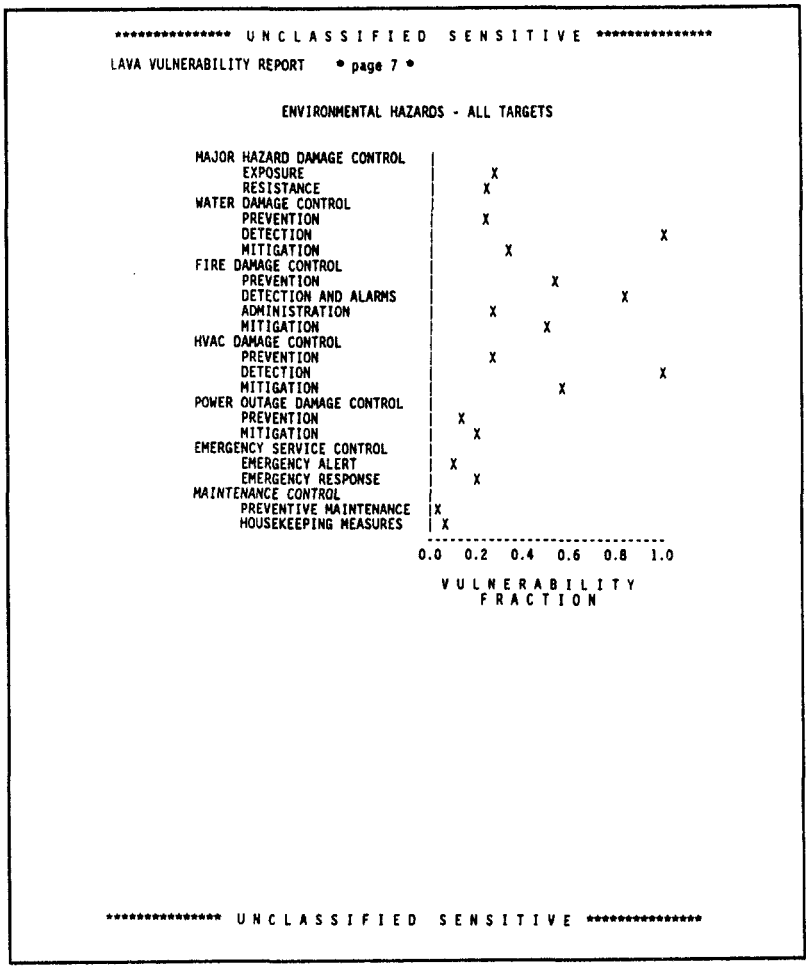
This report section summarizes the vulnerabilities as a function of the specific threat. The individual safeguards functions and subfunctions are listed with their normalized vulnerability score and the number of missing safeguards out of the total number of potential safeguards for the function. Please note, a low vulnerability score is better than a high score, and more safeguards are better than fewer safeguards.

```
********** UNCLASSIFIED SENSITIVE **********

LAVA/CS VULNERABILITY REPORT    * page 5 *

                    SUMMARY OF VULNERABILITIES
                     TO DIRECT HUMAN THREATS

ASSET           SAFEGUARD FUNCTION                VULNERABILITY SCORE (*)

FACILITY        ORGANIZATION REACHABILITY CONTROL
                  PERIMETER                       1.00 ( 20.00 out of  20)
                  BUILDING                        0.23 (  5.25 out of  23)
                  AREA                            1.00 ( 24.00 out of  24)
                  ROOM                            1.00 ( 38.00 out of  38)
                ORGANIZATION ACCESS CONTROL
                  GENERAL ACCESS                  0.15 (  8.50 out of  57)
                  VEND., SERV., VISITOR           0.29 ( 26.25 out of  89)
                  AUTHORIZATION                   0.21 (  9.00 out of  43)
                ORGANIZATION PERSONNEL MEASURES
                  MANAGEMENT AWARENESS            0.18 ( 14.75 out of  80)
                  EMP. STAT. MONITORING           0.26 (  6.00 out of  23)
                  SEC. & EMERG. TRAINING          0.18 (  9.00 out of  49)
                  EMERG. SERV. PERS. MONT.        0.32 ( 16.25 out of  51)
HARDWARE        HARDWARE REACHABILITY CONTROL
                  PERIMETER                       1.00 ( 20.00 out of  20)
                  BUILDING                        0.23 (  5.25 out of  23)
                  AREA                            1.00 ( 24.00 out of  24)
                  ROOM                            1.00 ( 38.00 out of  38)
                HARDWARE ACCESS CONTROL
                  PHYSICAL ACCESS                 0.20 (  9.00 out of  44)
                  VEND/SERV MAINT.                0.13 (  3.00 out of  23)
                  AUTHORIZATION                   0.07 (  4.00 out of  55)
                HARDWARE INVENTORY & BACKUP CONTROL
                  INVEN/AUDIT CONTROL             0.21 (  7.00 out of  33)
                  BACKUP CONTROL                  0.86 (  6.00 out of   7)
SOFTWARE        SOFTWARE REACHABILITY CONTROL
                  PERIMETER                       1.00 ( 20.00 out of  20)
                  BUILDING                        0.23 (  5.25 out of  23)
                  AREA                            1.00 ( 24.00 out of  24)
                  ROOM                            1.00 ( 38.00 out of  38)
                SOFTWARE ACCESS CONTROL
                  PHYSICAL ACCESS                 0.14 ( 13.00 out of  91)
                  LOGIN PROC.                     0.09 (  5.00 out of  55)
                  OP. SYST. PROC.                 0.14 (  7.00 out of  51)
                SOFTWARE APPLICATION CONTROL
                  SOFTWARE USE                    0.34 ( 17.00 out of  50)
                  DEV. & PROG. CHNG.              0.42 ( 14.00 out of  33)
                  ERR. PREV. & DETECTION          0.42 ( 17.00 out of  40)
                  CORRECTION & BACKUP             0.24 (  9.00 out of  37)
                SOFTWARE AUDIT CONTROL
                  INTERNAL AUDIT                  0.29 ( 16.00 out of  56)
                  DATA TRACEABILITY               0.04 (  1.00 out of  23)


********** UNCLASSIFIED SENSITIVE **********
```

Summary of Vulnerabilities of Specific Threats

3.4 Scatter Diagrams of Safeguards Functions

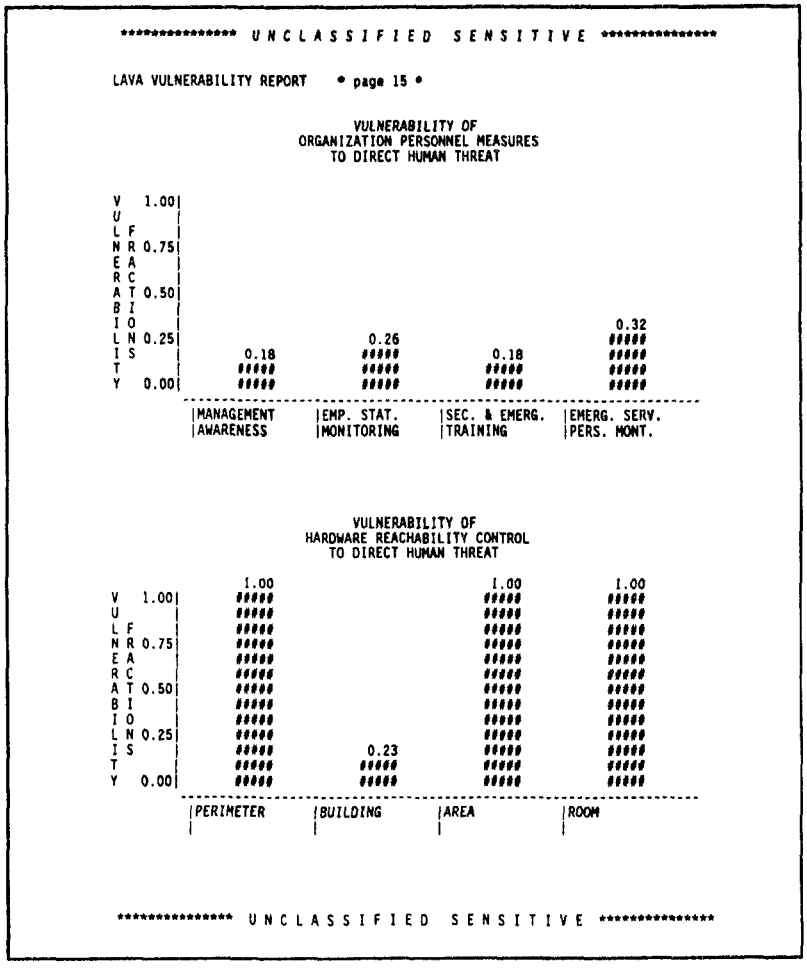
This report section shows plots of the individual threat/asset pairs. Natural or environmental hazards do not distinguish among assets; therefore all the targets are combined in the scatter diagrams as shown below. The scatter diagrams are pictorial representations of the two previously described tables. This visual representation allows management to determine rapidly the relative vulnerabilities of the computer safeguards system.



Scatter Diagrams of Safeguards Functions

3.5 Bar Charts of Individual Safeguards Functions

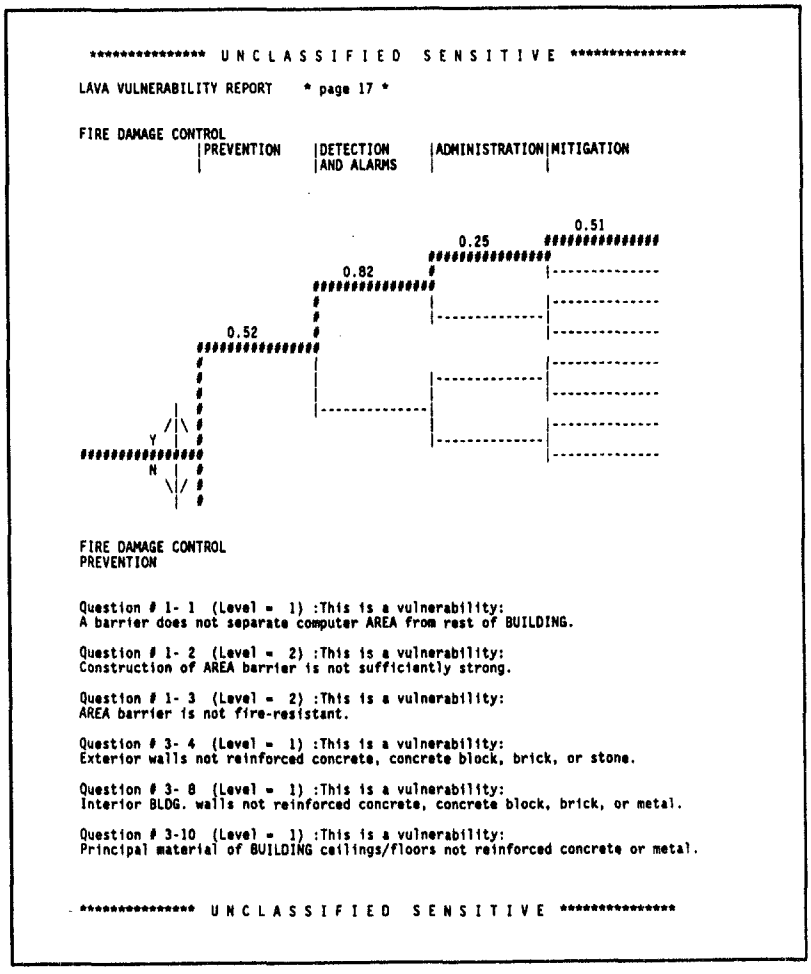
The bar charts in the report contain the same information shown in the scatter diagrams, but identify individual safeguards functions and subfunctions. These charts may be used to analyze a specific safeguards function in more detail.



Bar Charts of Individual Safeguards Functions

3.6 Detailed Plots of Event Trees with Listings of Vulnerabilities

Individual event trees for each specific safeguards function with their corresponding vulnerability fractions are plotted in this section of the report. Each question that indicated an absence of a safeguard is also listed for reference. A brief description of the specific vulnerability is printed to assist in interpreting the vulnerability assessment. This section is most useful to the individual responsible for improving the safeguards of the computer system.



Detailed Plots of Event Trees with Listings of Vulnerabilities

Chapter 4

THE DEMONSTRATION DISKETTE

4.1 About the Demonstration Diskette

The demonstration diskette gives you the feel of what it is like to perform a vulnerability assessment using the LAVA methodology. The demo, which takes about 15 minutes to complete, administers a short interactive questionnaire on one of two safeguards areas. You may select either area, and you may run the demo as often as you wish. Each question in the demonstration paraphrases the LAVA/CS questionnaire and represents a small subset of all questions included in LAVA/CS itself.

The LAVA/CS demonstration diskette will run on an IBM PC (or 100% compatible computer) with two floppy disk drives or a hard disk. You will also need a copy of MS DOS or PC DOS. The LAVA/CS package has been successfully used with versions 2.00 through 3.20. Because the demonstration produces some graphics, you will need both a graphics board and a graphics monitor to run the demonstration diskette successfully. You also will need to include in your `AUTOEXEC.bat` file the appropriate graphics commands for your graphics board.

First, install the diskette on your computer system. Installation instructions are provided in the next section of this user's manual. Once you have installed the demonstration diskette on your system, LAVA/CS will administer the interactive questionnaire, and you will be asked to answer questions relating to the safeguards area you have selected. After you have answered the questions, LAVA/CS will calculate the vulnerability scores and present

the vulnerability scores on the computer screen in both quantitative and linguistic forms. Next, LAVA/CS will list all missing safeguards for your review. Finally, a graphic representation of the event-tree structure for the chosen safeguards area will be plotted. Please note that, for demonstration purposes, the vulnerability score associated with the demonstration questions appears only on the last branch of the event-tree.

4.2 How to Install the Demonstration Diskette

There are two methods for preparing to run the LAVA/CS demo. If you have a computer with two floppy disk drives use METHOD 1. If your computer has a fixed/hard disk use METHOD 2.

The preparation for running the demo consists of expanding DOS's files and buffers to accommodate the demo package and copying your BASIC onto the demonstration diskette.

4.2.1 METHOD 1. For Dual Floppy Disk Drives

Note: The symbol <CR> means to depress the "Enter" key. Also, before beginning the actual demo, you must issue commands (if any) to turn on graphics board. (e.g. Ultra-Pak board commands are BIGSCR and MODEG).

1. Turn on computer and load operating system. (The LAVA/CS demo has been successfully demonstrated with versions 2.00 through 3.20 of MS or PC DOS.)

2. It is wise to make a backup copy of the demonstration diskette. Consult your DOS manual on how to do this.

3. Place your DOS diskette in Drive B.

4. Place a blank diskette labelled "Working Demo" into Drive A.

5. Format the blank diskette with the operating system on it by typing:

```
B:FORMAT A:/S     <CR>
```

6. Next, you must copy your BASIC onto the demonstration diskette. For example, if you have a genuine IBM PC or a COMPAQ, type:

```
COPY B:BASICA.com  A:      <CR>
```

If your system uses GWBASIC, type:

```
COPY B:BASICA.com  A:      <CR>

COPY B:GWBASIC.exe A:      <CR>
```

7. Remove the DOS diskette from Drive B and replace it with the demonstration diskette. Then type:

```
COPY B:CONFIG.SYS A:    <CR>
```

8. Reboot your computer system with the "Working Demo" in Drive A by placing the "Working Demo" into Drive A and depressing the control, alternate, and delete keys simultaneously.

9. You are now ready to begin the demonstration. Remove the "Working Demo" and place the demonstration diskette into drive A and type:

```
LAVA       <CR>
```

10. The LAVA/CS title screen should appear. Follow the directions appearing on the screen.

4.2.2 METHOD 2. For Fixed/Hard Disk

Note: The symbol <CR> means to depress the "Enter" key. Also, before beginning the actual demo, you must issue commands (if any) to turn on graphics board. (e.g. Ultra-Pak board commands are BIGSCR and MODEG).

1. Turn on computer and load operating system. (The LAVA/CS demo has been successfully demonstrated with versions 2.00 through 3.20 of MS or PC DOS.)

2. Log on to your hard disk (for example, Drive C) by typing:

```
C:       <CR>
```

   where C: is the drive specification of your fixed/hard disk.

3. *Either BASICA must be in this directory* or a PATH statement must be included in the AUTOEXEC.bat file so that BASICA is accessible (see your DOS manual for information about the PATH statement).

4. Change the DOS current directory (`CD` command) to the one which will contain the LAVA/CS Demonstration Package software, or make a new directory in which to store the software and log on to that directory.

5. Place the LAVA/CS Demonstration Package diskette in Drive A.

6. Copy the LAVA/CS Demonstration Package diskette by typing:

```
COPY A:*.*  C:      <CR>
```

   where `C:` is the drive specification of your fixed/hard disk.

7. Remove the LAVA/CS Demonstration Package diskette from Drive A.

8. IMPORTANT !!! You must have a `CONFIG.sys` file on your hard disk's root directory. The `CONFIG.sys` file must have assigned at least 20 files and at least 8 buffers.

```
files=20

buffers=8
```

   If you do not have a `CONFIG.sys` file, you may either create one that contains the above two lines or you may copy the `CONFIG.sys` file from the LAVA/CS Demonstration Package diskette.

9. Reboot your computer system.

10. You are now ready to run the LAVA/CS Demonstration Package. Change to the directory containing the demonstration and type:

```
LAVA       <CR>
```

11. The LAVA/CS title screen should appear. Follow the instructions that appear on the screen.

Part II

TUTORIAL

Chapter 5

THE LAVA/CS TUTORIAL

5.1 About the Tutorial

The Tutorial explains how to do a vulnerability assessment using the LAVA/CS software: it provides a quick reference for using the program. The tutorial will lead you through the installation of the LAVA/CS software and prepare you to answer the questionnaire and print the vulnerability reports.

There are four chapters in the Tutorial:

CHAPTER 5. THE LAVA/CS TUTORIAL - Chapter 5 contains information about the LAVA/CS tutorial and the hardware, software and operating system requirements needed to run LAVA/CS. This chapter also supplies information you will need to prepare to run LAVA/CS. It provides detailed instructions for making copies of the diskettes and for installing the software on your computer system.

CHAPTER 6. ANSWERING THE QUESTIONNAIRE - Chapter 6 explains how to run the interactive questionnaire.

CHAPTER 7. SCORING THE QUESTIONNAIRE - Chapter 7 provides information on how the vulnerability scores are calculated.

CHAPTER 8. PRINTING THE REPORT - Chapter 8 explains how to print the five vulnerability reports listed in Chapter 3.

Getting ready to use LAVA/CS on your personal computer is an easy two-step process–first, you will need to make back-up copies of the LAVA/CS diskettes and second, you will need to prepare your computer (configure your system) to run the LAVA/CS software.

Section 5.5 of the Tutorial explains in detail how to make back-up copies of the diskettes. Please check at this time to make sure you have all six LAVA/CS diskettes. You also will need six blank diskettes on which to copy the software (you do not need to copy the INSTALL diskette, but you will make two copies of the ANSWER diskette).

There are two methods for preparing your computer system to run the LAVA/CS program. If you have a computer with two floppy disk drives, please refer to Section 5.6 of the Tutorial for instructions. If your computer has a fixed/hard disk, Section 5.7 provides the necessary instructions.

5.2 The LAVA/CS Software – What You Have

The LAVA software consists of six (6) program diskettes. The diskettes are labeled:

1. ANSWER–The ANSWER diskette contains all the responses to the questionnaire. The answers to the questionnaire provide the information for scoring the vulnerability assessment and printing the LAVA/CS reports. If your computer system has two floppy disk drives, the ANSWER diskette will remain in drive A at all times during the assessment.

2. START–The START diskette contains information that will determine the classification level of the computer system under assessment. Responses to the questions asked by the START diskette are stored on the ANSWER diskette.

3. QUESTION–The QUESTION diskette contains the heart of the vulnerability assessment – the interactive questionnaire. Responses to the questions asked by this diskette are stored also on the ANSWER diskette.

4. SCORE–The SCORE diskette reads the answers contained on the ANSWER diskette and calculates the vulnerability scores.

5. REPORT–The REPORT diskette prints general summary and detailed reports.

6. INSTALL–The INSTALL diskette contains the necessary computer instructions for installing the LAVA/CS software on your hard or fixed

disk. You will need to use this diskette only if you plan to install LAVA/CS on your hard or fixed disk.

If you do not have each of the six diskettes, please contact us immediately. The Where to Get Help section (Appendix G) of this manual contains the necessary phone number and address.

IMPORTANT !!!

We recommend that you make back-up copies of all the appropriate LAVA/CS software diskettes. These diskettes are not copy protected. Detailed instructions for backing up the diskettes are included in this tutorial. You also may consult your DOS manual for instructions.

The LAVA/CS software places all your responses to the questionnaire onto the ANSWER diskette. When you are running the program, this diskette must be in drive A at all times. Because the ANSWER diskette contains all responses to the questionnaire, it is crucial to the successful completion of the vulnerability assessment. Therefore, we urge you to make a back-up copy of this diskette on a regular basis.

Both the core team and the transient team should be present to answer the questions contained on the START and QUESTION diskettes. It is important that the assessment team reach a consensus before ANY response to a question is entered into the computer. Only the lead assessor need be present when SCORE and REPORT diskettes are run.

5.3 Hardware/Software Requirements

The minimum hardware configuration needed to run the LAVA/CS software is

1. IBM PC, or IBM PC XT, or 100% compatible computer.
2. 512KB of memory.
3. One floppy disk drive AND one other storage medium (either a floppy disk drive or a fixed/hard disk).
4. IBM ProPrinter, Epson FX-80 printer, or 100% compatible printer.

Most of the LAVA/CS software was written in the dBaseIII programming language and is furnished to you in compiled form. The only software you

need to run LAVA/CS is a copy of MS DOS or PC DOS. The LAVA/CS package has been tested using PC version 3.10, although it has been operated successfully with with MS DOS versions 2.00 through 3.20.

5.4 What You Need to Begin Installing the LAVA/CS Software

Getting ready to use LAVA/CS on your personal computer is easy. First, you will need to make back-up copies of the appropriate LAVA/CS diskettes– Section 5.5 of this chapter explains how to do this. Please check at this time to make sure you have all six LAVA/CS diskettes. If you do not have each of the diskettes, please consult the Appendix G of the manual. You also will need six blank diskettes on which to copy the LAVA/CS software (the ANSWER diskette will be copied twice).

Next, you will need to prepare your computer to run the software. There are two methods for doing so. If you have a computer with two floppy disk drives, please refer to Section 5.5 and 5.6 for installation instructions. If your computer has a fixed/hard disk or one floppy disk drive and a hard disk, Section 5.7 provides the instructions.

5.5 How to Make Copies of the LAVA/CS Diskettes

If you have a computer system with dual floppy disk drives you will need to make copies of the LAVA/CS diskettes. It is very important that you copy the LAVA/CS diskettes. To begin the process you will need all LAVA/CS diskettes (with the exception of the INSTALL diskette) and six blank diskettes. These instructions will assist you in making two copies of the ANSWER diskette and one copy of each of the other four LAVA/CS diskettes. Once all copies have been made, we suggest you put the master copies of the LAVA/CS diskettes away for safekeeping and future reference.

NOTE: In the following instructions the "Return" or "Enter" key is referred to by the symbol <CR>. Please press this key when you see <CR> indicated in the tutorial.

To Label and Format Blank Diskettes

1. Prepare six labels that read:

```
START
Copied:     "current date"
System:     "name of your system"
Assessor:   "your name"

ANSWER
Copied:    "current date"
System:    "name of your system"
Assessor: "your name"

ANSWER (BACK-UP)
Copied:     "current date"
System:     "name of your system"
Assessor:   "your name"

QUESTION
Copied:     "current date"
System:     "name of your system"
Assessor:   "your name"

SCORE
Copied:     "current date"
System:     "name of your system"
Assessor:   "your name"

REPORT
Copied:     "current date"
System:     "name of your system"
Assessor:   "your name"
```

2. Place one of the labels on each of the blank diskettes.
3. You will now begin to format each of the six blank diskettes.
4. Place your DOS diskette into drive A and type:

```
FORMAT B:/V <CR>
```

Next, follow the directions that appear on the screen. When the computer asks for a volume name for each of the diskettes type the name of the diskette. For example, type :

```
START      <CR>
```

NOTE: Your computer may ask if you would like to format another diskette. Answer in the affirmative. For example, the following might appear on your computer screen :

```
Format another diskette (Y/N)?
```

You would respond by typing

```
Y          <CR>
```

Repeat this process for each of the remaining LAVA/CS diskettes.

5. Once all six diskettes have been formatted, remove the DOS diskette from drive A.
6. You are now ready to begin copying the diskettes.

To Copy the START Diskette

1. Place the blank diskette labeled START into drive B.
2. Place the master copy of the START diskette into drive A and type:

```
COPY A:*.* B: <CR>
```

3. After the copying process has been completed, remove the diskettes from drive A and drive B.
4. You are ready to copy the next LAVA/CS diskette.

To Copy the ANSWER Diskettes

1. You will make two copies of the ANSWER diskette. One will be labeled ANSWER and the other, ANSWER (BACK-UP).

2. Place your DOS system diskette into drive A.
3. Place the blank diskette labeled ANSWER into drive B.
4. Copy one DOS file from the DOS diskette in drive A to the blank ANSWER diskette in drive B by typing:

```
COPY \COMMAND.COM B:    <CR>
```

5. After the file, COMMAND.com, has been copied, remove the DOS diskette from drive A. Place the master copy of the ANSWER diskette into drive A. The new copy of the ANSWER diskette still should be in drive B.
6. Copy all files from the master copy in drive A to the new copy in drive B by typing:

```
COPY A:*.* B:       <CR>
```

7. After the copying has been completed, remove the master copy from drive A.
8. The newly copied diskette labeled ANSWER should be in drive B. Place the blank diskette labeled ANSWER (BACK-UP) into drive A. Make the back-up copy of the ANSWER diskette by typing

```
COPY B:*.*  A: <CR>
```

9. Remove the newly copied back-up ANSWER diskette from drive A.
10. Remove the copy of the ANSWER diskette from drive B. DO NOT place a write protect tab on either of the ANSWER diskettes.
11. You are now ready to copy the next LAVA/CS diskette.

To Copy the QUESTION Diskette

1. Place the blank diskette labeled QUESTION into drive B.
2. Place the master copy of the QUESTION diskette into drive A and type:

```
COPY A:*.* B: <CR>
```

3. After the copying process has been completed, remove the diskettes from drive A and drive B. Place a write-protect tab over the notch on the right side of each diskette.

4. You are ready to copy the next LAVA/CS diskette.

To Copy the SCORE Diskette

1. Place the blank diskette labeled SCORE into drive B.

2. Place the master copy of the SCORE diskette into drive A and type:

```
COPY A:*.* B: <CR>
```

3. After the copying process has been completed, remove the diskettes from drive A and drive B. Place a write-protect tab over the notch on the right side of each diskette.

4. You are ready to copy the next LAVA/CS diskette.

To Copy the REPORT Diskette

1. Place the blank diskette labeled REPORT into drive B.

2. Place the master copy of the REPORT diskette into drive A and type:

```
COPY A:*.* B: <CR>
```

3. After the copying process has been completed, remove the diskettes from drive A and drive B. Place a write-protect tab over the notch on the right side of each diskette.

4. You are ready to run LAVA/CS.

5.6 Configuring a Computer with Two Floppy Disk Drives

1. Insert a copy of your PC's DOS diskette into drive A.
2. Turn on the computer.
3. Turn on the printer.
4. Wait for the computer to perform its system check. If your computer displays the message,

   ```
   Enter new date
   ```

   then you either do not have a clock card installed or it is not active. Follow instructions 5 and 6. If your computer does not display the above message, skip instructions 5 and 6 and proceed with instruction 7.
5. Enter the current date. For example, if today is Tuesday, July 21, 1987 then type:

   ```
   07-21-87 <CR>
   ```

   NOTE: We use the notation

   ```
   <CR>
   ```

   to indicate a carriage return.
6. Enter the current time. For example, if it is 2:15 pm, then type:

   ```
   14:15 <CR>
   ```
7. To run LAVA/CS you need a "working" copy of MS or PC DOS (do not use your DOS distribution diskette). The LAVA/CS package has been used successfully with versions 2.00 through 3.20. To determine which DOS version you have, either obtain the information from the computer screen or type:

   ```
   ver <CR>
   ```

8. Next, you will need to configure your system software. Every time an IBM PC or compatible starts up (boots), it checks for a file called `CONFIG.sys`. This file resides in your root directory and contains information your PC uses to set up the way it operates. You must have a `CONFIG.sys` file in your root directory to use LAVA. (If you do not know what a root directory is, please refer to your MS DOS or PC DOS manual.)

   To determine if your DOS diskette has a `CONFIG.sys` file on it, type:

   ```
   DIR *.SYS <CR>
   ```

   If your DOS diskette has a `CONFIG.sys` file, go to instruction 9 and skip instruction 10. If your DOS diskette does not have a `CONFIG.sys` file, skip instruction 9 and go to instruction 10.

9. If you have the `CONFIG.sys` file, you will need to determine if it provides for at least the minimum number of files and buffers needed to run LAVA/CS. Display the contents of the `CONFIG.sys` file by typing:

   ```
   TYPE CONFIG.SYS <CR>
   ```

   The `CONFIG.sys` file should contain the lines

   ```
   FILES = 20

   BUFFERS = 22
   ```

   The `CONFIG.sys` file must have assigned at least 20 files and at least 22 buffers. If you must increase the values, use either the line editor (`EDLIN`) that comes with the DOS system diskette or use the editor of your choice. Please refer to their manuals for editing instructions.

   If the number of files and buffers assigned in your `CONFIG.sys` file is greater than 20 and 22, respectively, you do not need to make any change.

10. If your DOS diskette does not have a `CONFIG.sys` file, you can create one by typing the following four lines. Each of the lines is followed by a carriage return:

```
COPY CON: CONFIG.SYS <CR>
FILES = 20           <CR>
BUFFERS = 22         <CR>
^Z                   <CR>
```

NOTE: ^Z means to press Z while holding down the Ctrl key. You may wish to check to ensure the CONFIG.sys file was created. You can do this by typing

```
DIR *.SYS      <CR>
```

Your computer will respond by listing all files in your directory ending with .SYS; check to see if the CONFIG.sys file was created. If the file was created, proceed to instruction 11. If the file was not created, repeat the process described in instruction 10.

You may wish to check the contents of the CONFIG.sys file. You can do so by typing

```
TYPE CONFIG.SYS      <CR>
```

Your computer will respond by displaying the contents of the file.

11. You have now configured your computer system to run LAVA/CS.

5.7 Installing LAVA/CS on a Computer with a Hard/Fixed Disk

1. Turn on your computer.
2. To run LAVA/CS you need a "working" copy of MS or PC DOS (do not use your DOS distribution diskette). The LAVA/CS package has been used successfully with versions 2.00 through 3.20. To determine which DOS version you have, either obtain the information from the computer screen or type:

```
ver <CR>
```

3. Next, you will need to configure your system software. Every time an IBM PC or compatible starts up (boots), it checks for a file called `CONFIG.sys`. This file resides in your root directory and contains information your PC uses to set up the way it operates. You must have a `CONFIG.sys` file in your root directory to use LAVA. (If you do not know what a root directory is, please refer to your MS DOS or PC DOS manual.)

   To determine if your DOS diskette has a `CONFIG.sys` file on it, type:

   ```
   DIR *.SYS <CR>
   ```

   If your DOS diskette has a `CONFIG.sys` file, go to instruction 4 and skip instruction 5. If your DOS diskette does not have a `CONFIG.sys` file, skip instruction 4 and go to instruction 5.

4. If you have the `CONFIG.sys` file, you will need to determine if it provides for at least the minimum number of files and buffers needed to run LAVA/CS. Display the contents of the `CONFIG.sys` file by typing:

   ```
   TYPE CONFIG.SYS <CR>
   ```

   The `CONFIG.sys` file should contain the lines

   ```
   FILES = 20

   BUFFERS = 22
   ```

   The `CONFIG.sys` file must have assigned at least 20 files and at least 22 buffers. If you must increase the values, use either the line editor (`EDLIN`) that comes with the DOS system diskette or use the editor of your choice. Please refer to their manuals for editing instructions.

   If the number of files and buffers assigned in your `CONFIG.sys` file is greater than 20 and 22, respectively, you do not need to make any change.

5. If your DOS diskette does not have a `CONFIG.sys` file, you can create one by typing the following four lines. Each of the lines is followed by a carriage return:

```
COPY CON: CONFIG.SYS <CR>
FILES = 20           <CR>
BUFFERS = 22         <CR>
^Z                   <CR>
```

NOTE: ^Z means to press Z while holding down the Ctrl key. You may wish to check to ensure the CONFIG.sys file was created. You can do this by typing

```
DIR *.SYS      <CR>
```

Your computer will respond by listing all files in your directory ending with .SYS; check to see if the CONFIG.sys file was created. If the file was created, proceed to instruction 6. If the file was not created, repeat the process described in instruction 5.

You may wish to check the contents of the CONFIG.sys file. You can do so by typing

```
TYPE CONFIG.SYS      <CR>
```

Your computer will respond by displaying the contents of the file.

6. You will need 1.2 megabytes of free disk space to install the software on your hard/fixed disk. First, determine if there is sufficient storage space on your hard disk for the LAVA/CS software. This can be done by changing the default drive to the hard disk (see your DOS manual for instructions on how to change the default drive) and typing:

   ```
   DIR <CR>
   ```

   The computer will list all files and directories residing on the disk. The amount of available disk space follows the list of files. If you have sufficient disk space, follow instructions 7, 8, 9, and 11 below.

   If you do not have enough space on your hard disk, you will need to remove files from your hard disk until you have a minimum of 1.2 megabytes (1,200,000 bytes) of free disk space or you may use another computer system with sufficient disk space.

7. Insert the diskette labeled INSTALL in drive A.

8. Log on to the hard/fixed disk (we will use C: as the designated drive) by typing:

   ```
   C:    <CR>
   ```

9. The computer will respond with `C>`. Type:

   ```
   A:    <CR>
   ```

   then type:

   ```
   INSTALL <CR>
   ```

10. Follow the instructions appearing on your monitor.

11. LAVA/CS has been installed on your hard disk. If the installation has been completed successfully, the following prompt should appear on your computer screen:

    ```
    C:\lava>
    ```

Chapter 6

ANSWERING THE QUESTIONNAIRE

6.1 Initializing the Questionnaire

1. Place the diskette labeled ANSWER in drive A. Place the diskette labeled START in drive B.

2. If your computer system has two floppy disk drives, change the default drive to drive B by typing:

   ```
   B:      <CR>
   ```

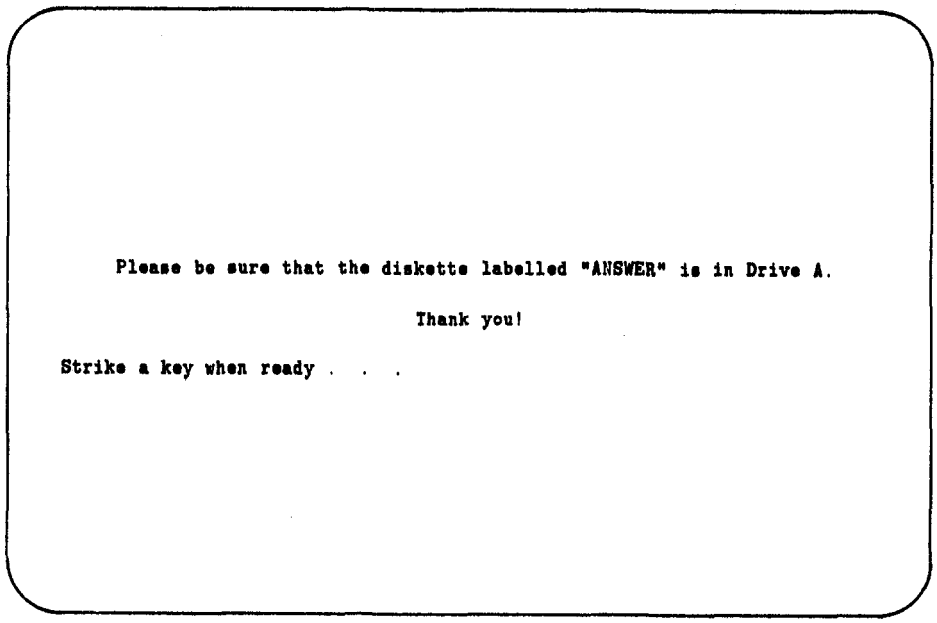
   NOTE: Hard disk users will need to ensure that they have designated the hard disk as their default drive and are in the LAVA subdirectory.

3. Now type:

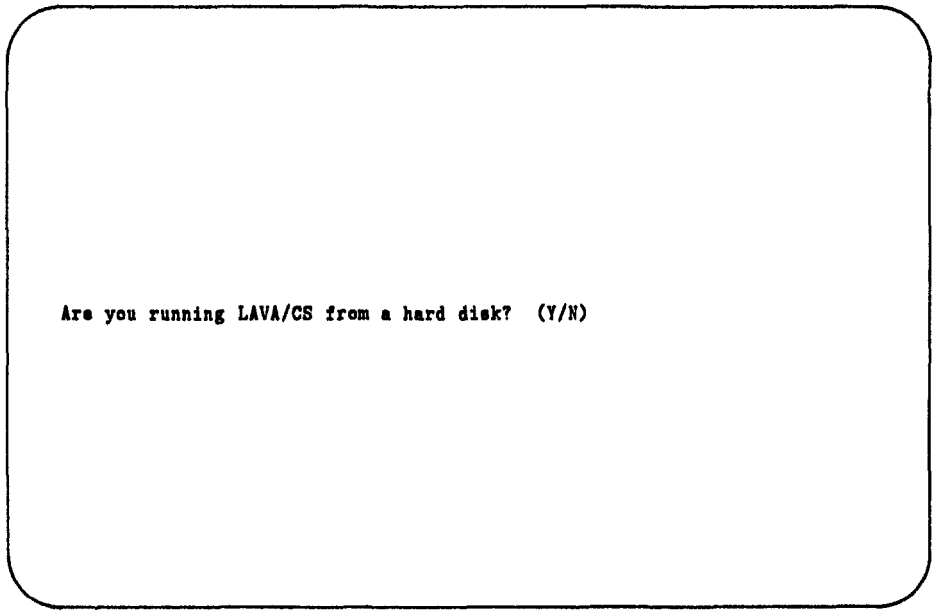
   ```
   START <CR>
   ```

   (screens 6.1 - 6.2)

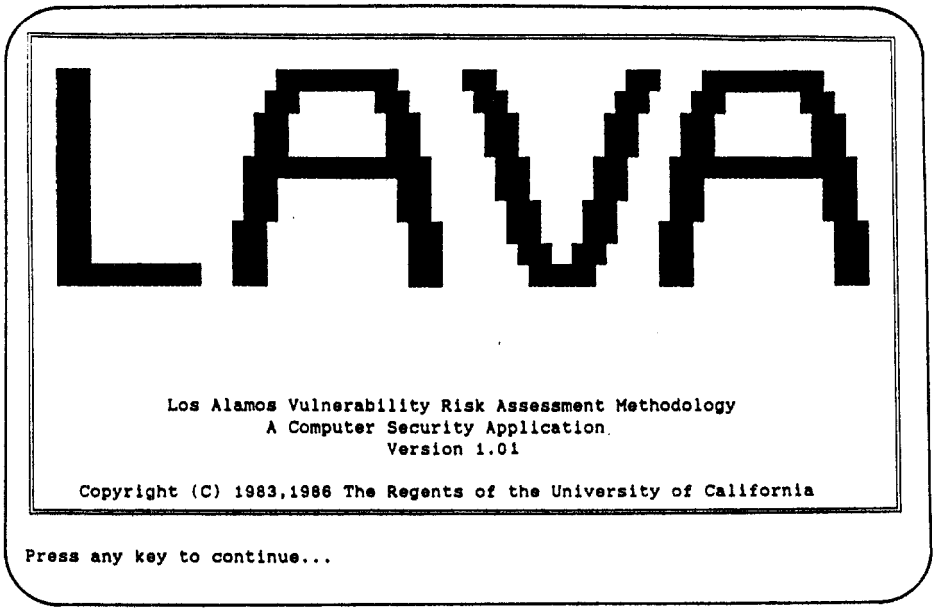
4. The program will ask you if you are running LAVA/CS from a hard disk (see Screen 6.2). Respond to this question as is appropriate. The program will present acknowledgments on the screen. (screens 6.4 - 6.7)



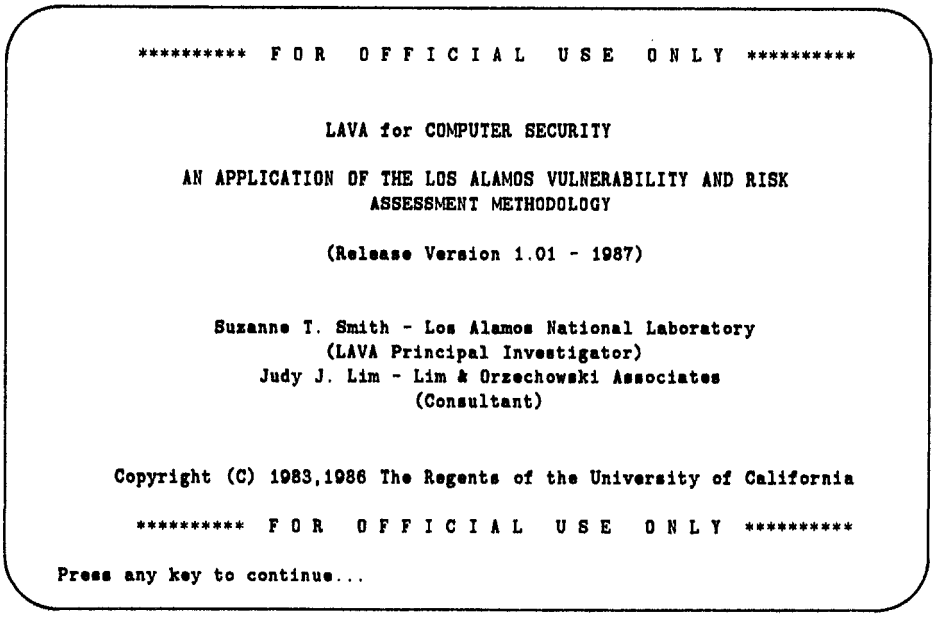
Screen 6.1



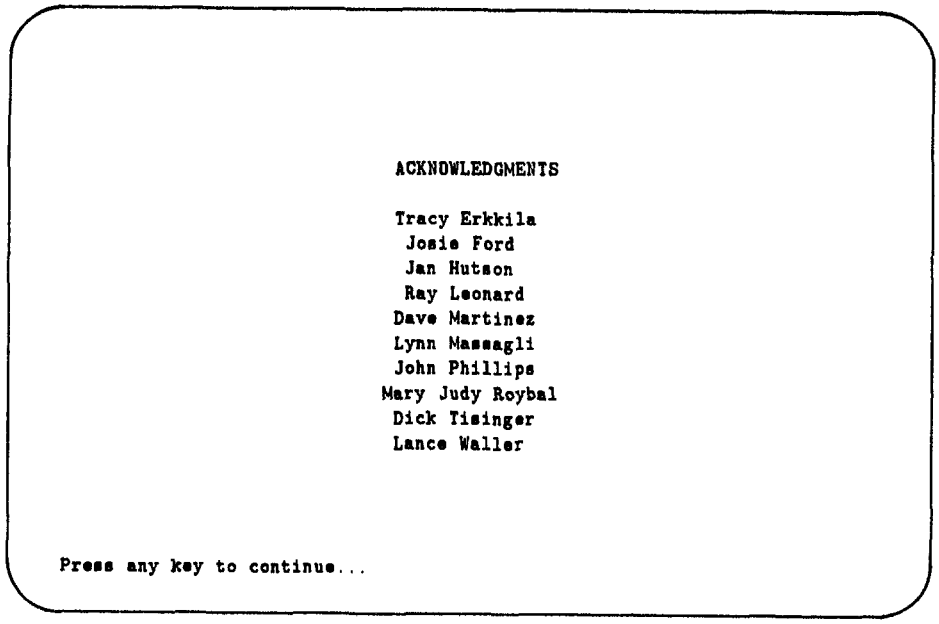
Screen 6.2



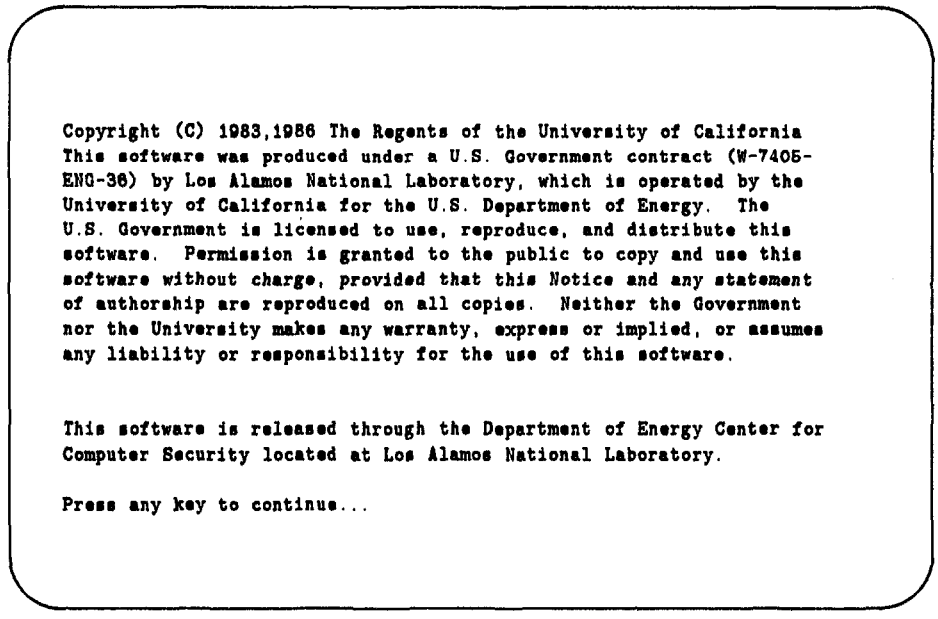
Screen 6.3



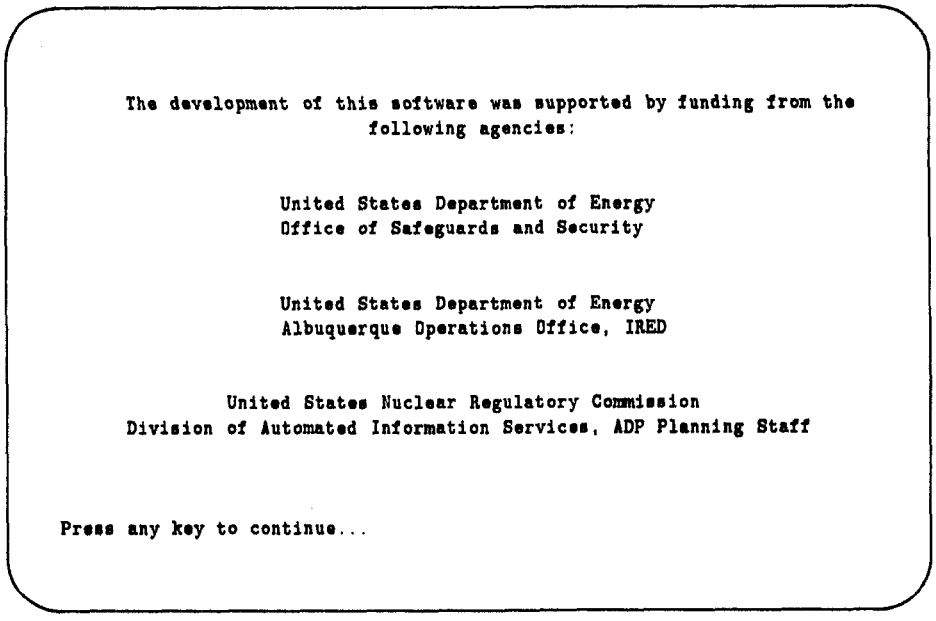
Screen 6.4



Screen 6.5

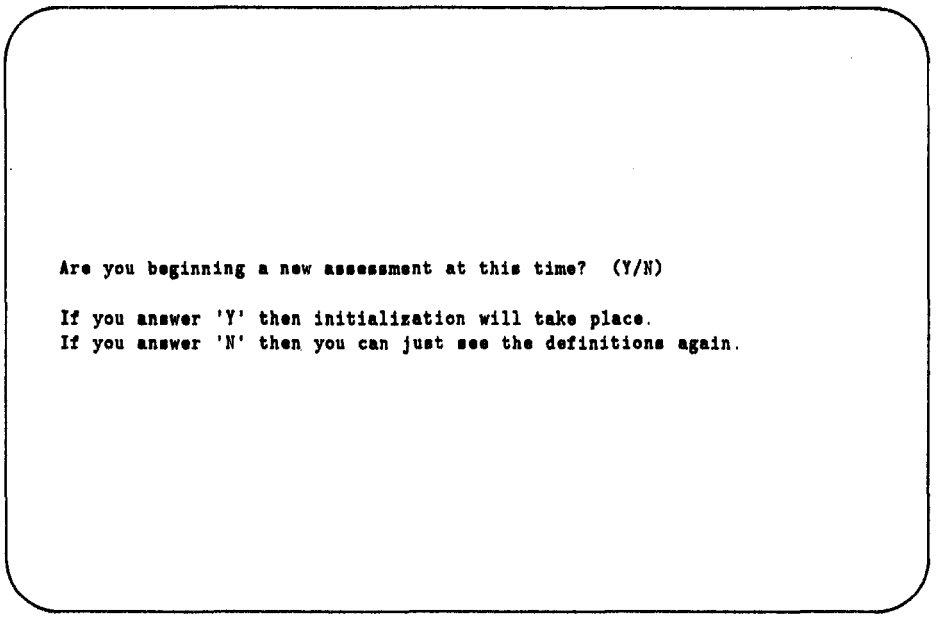


Screen 6.6


The development of this software was supported by funding from the following agencies:
United States Department of Energy
Office of Safeguards and Security
United States Department of Energy
Albuquerque Operations Office, IRED
United States Nuclear Regulatory Commission
Division of Automated Information Services, ADP Planning Staff
Press any key to continue...

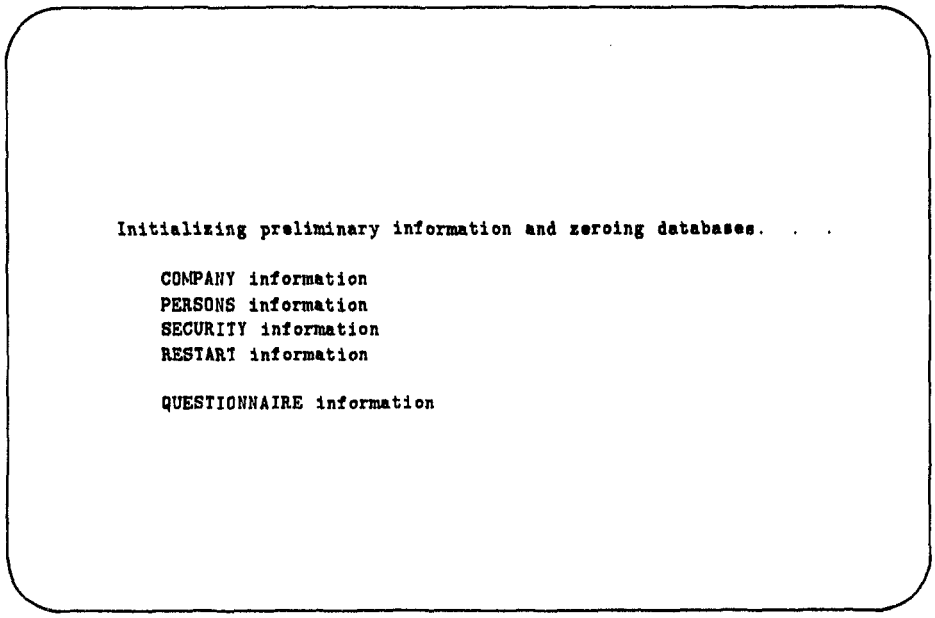
Screen 6.7

5. You will be asked if you are beginning the assessment for the first time. If you are beginning the assessment for the first time, enter "Y". If you are resuming the assessment, enter "N".



Screen 6.8

6. The LAVA/CS software will begin its initialization process next. The initialization process will take a few minutes to complete.



Screen 6.9

7. Next, you will see the definitions for the terms that are used throughout the interactive questionnaire. It is important for the assessment team to read and understand these definitions.

```
At this time, we provide an assortment of definitions for terms that have
been used throughout this methodology.  In addition, and VERY IMPORTANT,
you will receive instructions for answering the questionnaire that follows.

From the following definitions for FACILITY, ORGANIZATION, ENVIRONMENT,
PERIMETER ZONE, BUILDING, AREA, COMPUTER ROOM, and COMPUTER SYSTEM, the
assessment team should reach a consensus on the boundaries of these items
relative to the team's facility, procedures, and physical plant.

 ************************************************************************
 * The team should make a sketch of the installation clearly showing  *
 * these boundaries and display it prominently throughout the         *
 * assessment period.                                                 *
 ************************************************************************


PLEASE NOTE: These definitions and a clear understanding of them are VERY
important to executing LAVA/CS properly.  Please read them
carefully NOW and think about how they apply to you.

Press any key to continue...
```

Screen 6.10

The ORGANIZATION is the term we use for site or facility management and employees. It should be thought of as the largest possible organizational unit at the site or facility. It is NOT simply the group of persons who are responsible for the operation of the data center and data-center activities. In the case of organizations encompassing more than one site, the definition of ORGANIZATION is restricted to only one site and its activities. For example, the National Bureau of Standards is an organization that encompasses several sites. The site located in Gaithersburg, MD, has several data-processing installations and several sub-organizations. In LAVA/CS's context, the ORGANIZATION is the National Bureau of Standards - Gaithersburg.

The FACILITY is the term we use to describe all buildings, land, support activities and equipment (heating, air conditioning, power, water, and so forth), employees, supplies and property, information, and procedures and practices that the ORGANIZATION has under its control. Thus, to continue our National Bureau of Standards example, the FACILITY is everything located at the National Bureau of Standards' Gaithersburg site.

Press any key to continue...

Screen 6.11

The ORGANIZATION'S ENVIRONMENT is the physical environment of the ORGANIZATION controlling a (or several) data-processing installation(s). It may include several buildings, their surrounding grounds (if any), necessary operations equipment, and procedures established by the ORGANIZATION for dealing with both normal operations and emergencies. NOT restricted only to places in which the actual information processing goes on, the ENVIRONMENT includes buildings (and surrounding grounds) in which information about, processed by, or related to the information-processing center and the ORGANIZATION exists IN ANY FORM. The ENVIRONMENT includes policies and procedures established by the ORGANIZATION, support hardware for the computer center (power, heating, air conditioning, etc.,), and issues relating to the physical plant, personnel, and security.

The ORGANIZATION's grounds and buildings may be delimited by a PERIMETER ZONE that may or may not be fenced. In the case of ORGANIZATIONs having extensive land and several separate sites whose perimeter-zone access is controlled individually by site, this definition includes ONLY the area physically associated with each individual site.

Press any key to continue...

Screen 6.12

```
The BUILDING is the specific structure(s) housing the data-processing
installation.  It includes all buildings that house information-related
activities described in the definitions of AREA, ROOM, and SYSTEM.

The COMPUTER AREA includes locations where computer-related activities
take place and where information considered by the ORGANIZATION to be
sensitive or worthy of protection is held, processed, or stored.  Not nec-
essarily contiguous to the computer room, it may contain user work areas,
office space, laboratories, input/program keying areas, storage areas,
places for submitting input to the computer(s) or to data/input staff,
places to retrieve and peruse output, remote terminals, document
libraries, microfilm-processing equipment, microfilm/microfiche readers,
and similar or related things.

The COMPUTER ROOM is a partitioned space housing information-processing
(computer) equipment and related equipment.  This may include some or
all of the following:  media vaults, telecommunications closets, office
space for system personnel, maintenance workshops, and storage space for
related supplies.  Unless the tape library is specifically mentioned in a
question, consider the TAPE LIBRARY as part of the COMPUTER ROOM when
answering most questions.
Press any key to continue...
```

Screen 6.13

```
The COMPUTER SYSTEM encompasses both the computer-related machinery and the
storage media upon which information (programs, data, results, etc.)
is stored.

In the questionnaire, we may use COMPUTER INSTALLATION, COMPUTER CENTER,
or DATA CENTER interchangeably to mean the particular computer or set
of computers, related equipment, physical surroundings, and procedural
environment that we are assessing today.


The ADVERSARY is a person or persons who wants to acquire, damage, or
destroy the facility's assets.  The adversary can be an outsider, an
employe, a visitor, a contractor --- nobody is ruled out.


Press any key to continue...
```

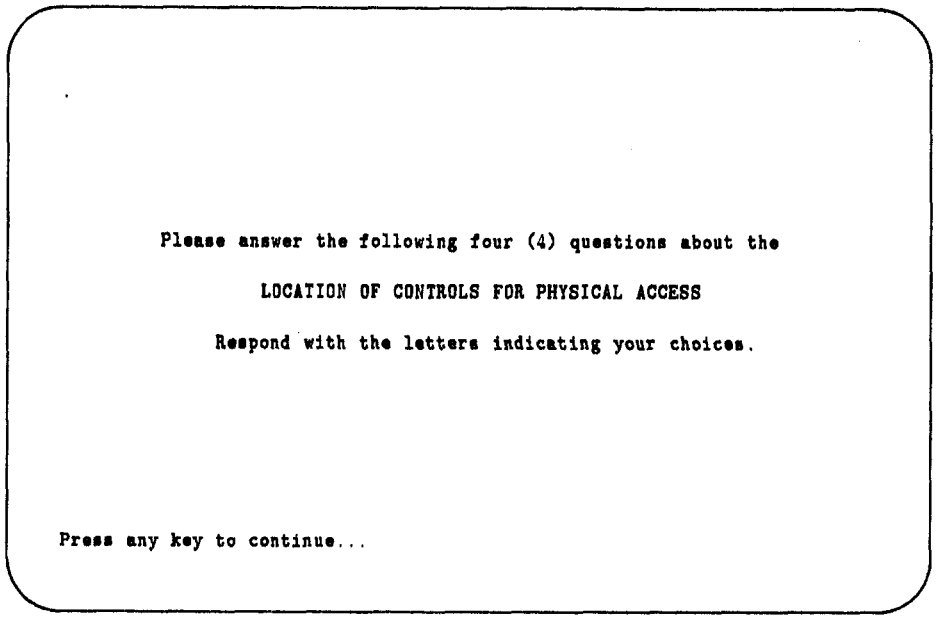
Screen 6.14

8. You will be asked to define the environment at your facility. It is essential for the entire assessment team to reach a consensus regarding these definitions. Please take your time deciding upon the definitions–they will affect your responses to questions asked later on in the questionnaire. When the assessment team has reached agreement, type in the boundary definitions as you are prompted by LAVA/CS.

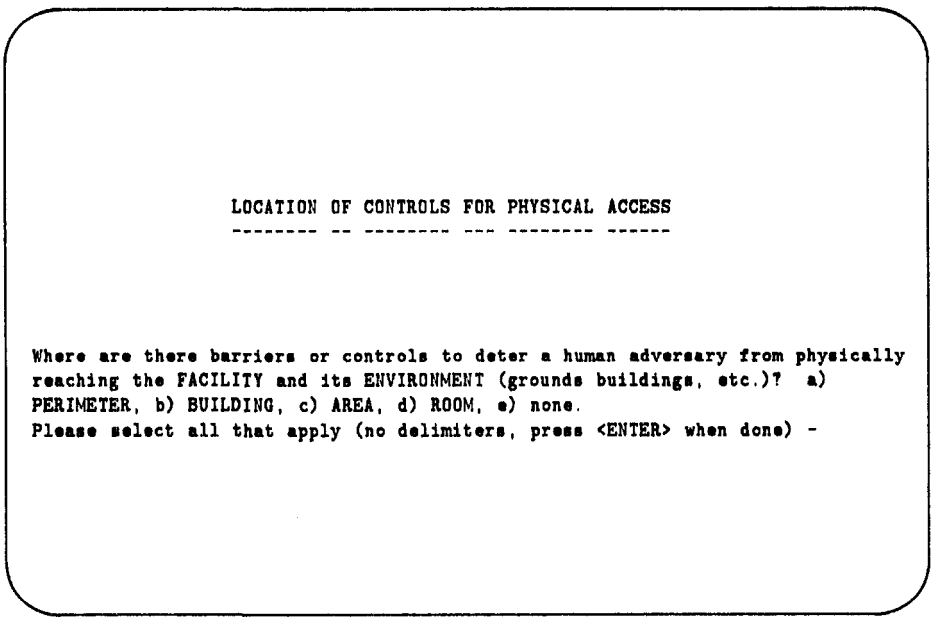
```
By now you have read the definitions for PERIMETER, BUILDING, AREA, and
ROOM. It is essential for the entire assessment team to reach a consensus
about how these definitions relate to the environment at YOUR facility in
bounding the assessment. Please take your time in deciding this issue --
it affects the way you will answer the questionnaire later. When the team
has reached agreement, type in the boundary definitions as LAVA/CS prompts
you for the following:

1) PERIMETER: exterior boundary of facility grounds

2) BUILDING : identity of specific building(s) housing computer(s)
or computer-related activities, equipment, and info.

3) AREA : outer boundaries of places having computer-related
activities, equipment, or information in any form

4) ROOM : specific room(s) housing the computer(s), computer
hardware, tape library, and media storage

Please limit your definitions to 80 or fewer characters.


Press any key to continue...
```

Screen 6.15

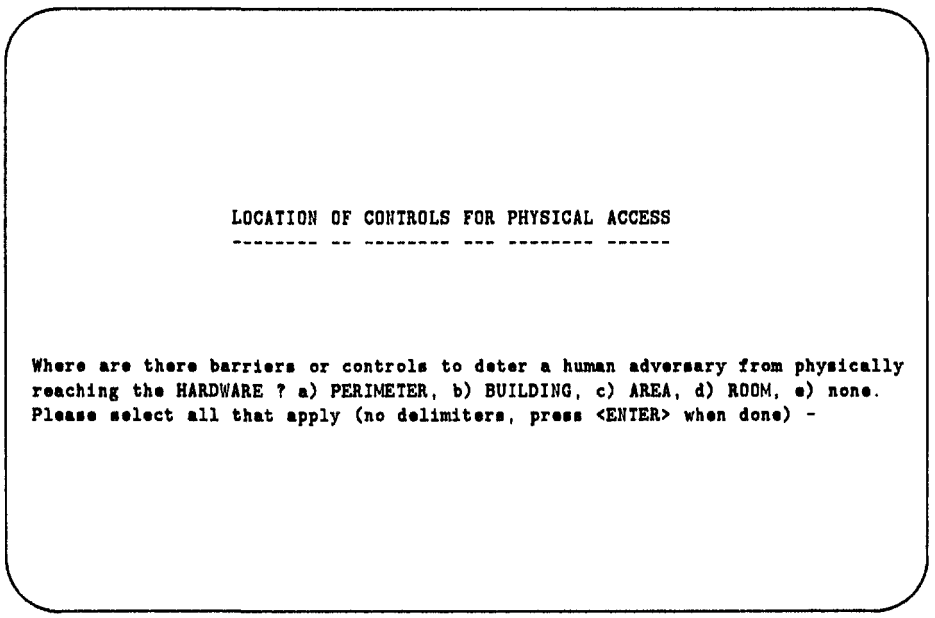
9. LAVA/CS will ask you questions regarding the reachability of the facility under assessment. Please respond to these questions as appropriate to your facility.



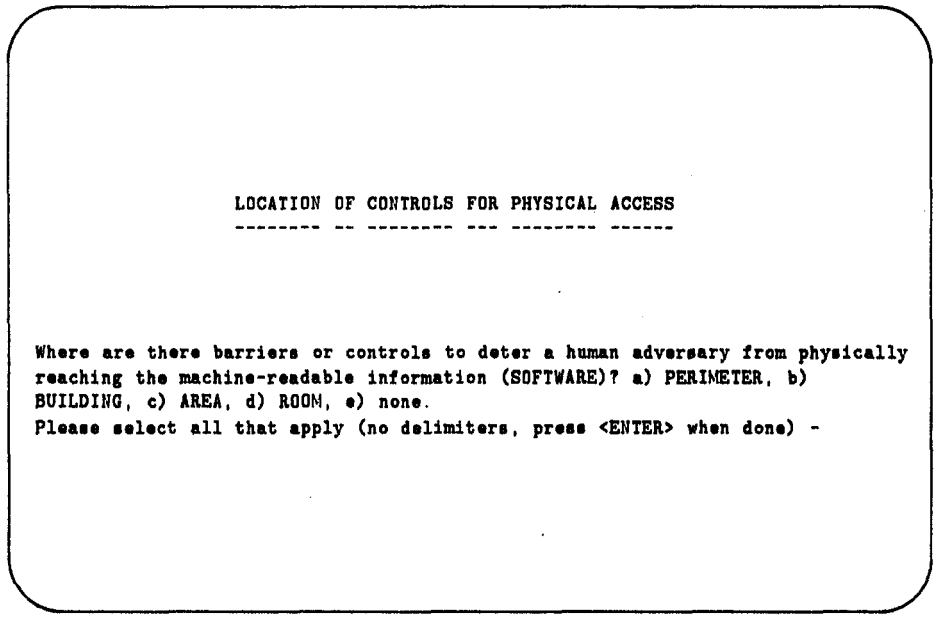
Screen 6.16



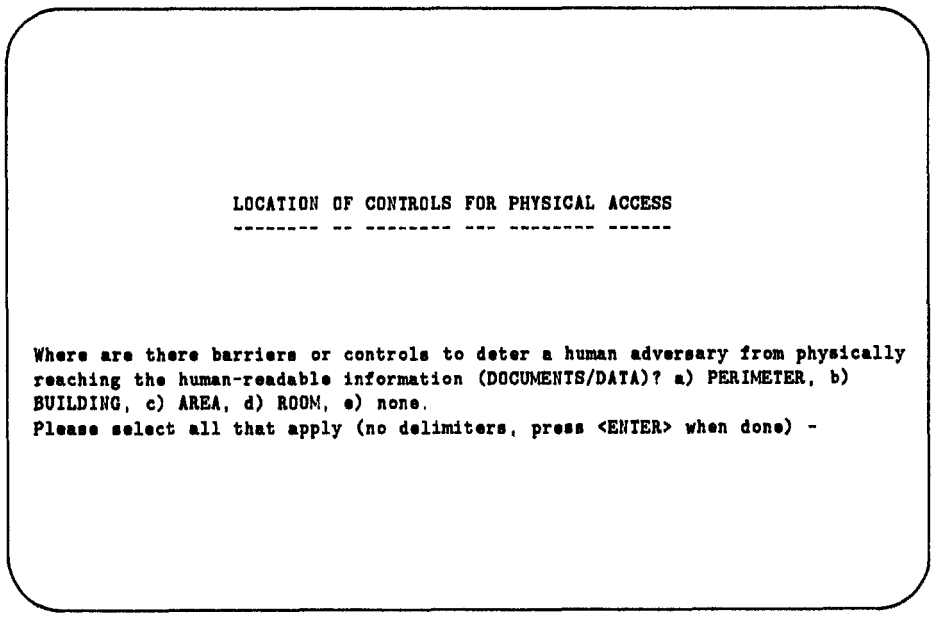
Screen 6.17



Screen 6.18

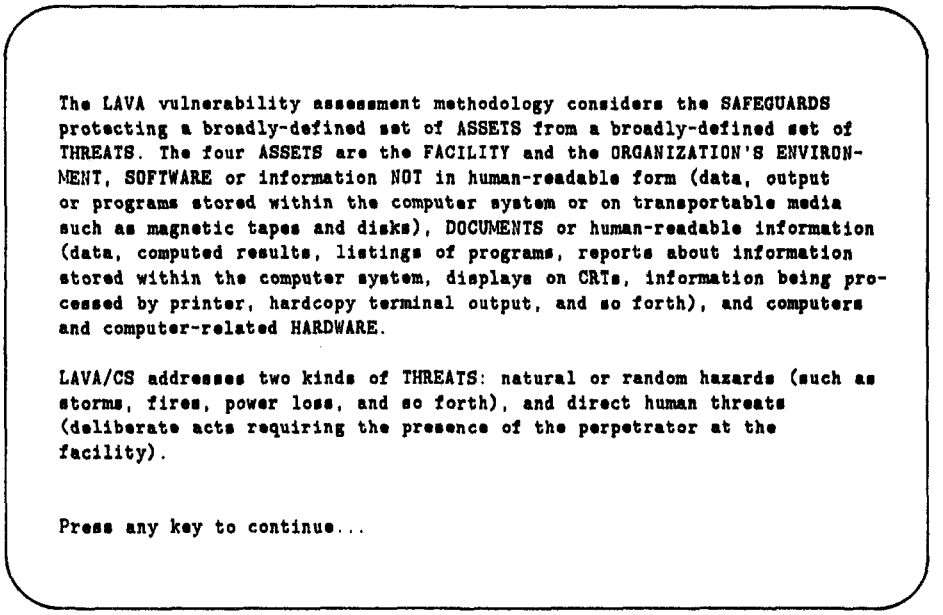


Screen 6.19



Screen 6.20

10. Next, LAVA/CS presents information regarding safeguards and threats and suggests items you may need for reference purposes while performing this assessment.



Screen 6.21

```
The SAFEGUARDS are broken down into FUNCTIONS to be performed by ELEMENTS
whose adequacy is characterized by ATTRIBUTES. An example FUNCTION might be
perimeter reachability control. ELEMENTS of this function might be fences
or guards (how the control is attained). ATTRIBUTES of the fence element
might include whether it is a specified minimum height, whether it has
added deterrents (like barbed wire or razor tape) on the fence, and whether
the fence has monitors and alarms that transmit to a place from which action
can be taken.

LAVA/CS's vulnerability assessment report itemizes BY FUNCTION the missing
safeguards for preventing the threats from succeeding against the targets.


Press any key to continue...
```

Screen 6.22

```
The following items may be needed for reference purposes:

1) A scale floor plan of the computer ROOM and AREA showing the locations
of all doors, windows, attached offices, user work areas, supply
rooms, media storage rooms, communications closets, and specific pieces
of the larger system hardware, the locations of all ceiling and under-
floor smoke detection devices and manually-operated alarm switches, fire
extinguishers, emergency lights, the locations of all water-detection
devices, the locations of monitors, alarms, motion detectors, CCTV cameras,
and recording devices, the locations of all guard stations, and the kinds
and locations of devices to verify and authenticate personnel identity.

2) A copy of the 'Computer Center Emergency Response Plan.'

3) A list of the more important pieces of information stored in non-human
readable form within the computer system (SOFTWARE).

4) A list of important pieces of information kept in human-readable form
for use at the facility (DOCUMENTS AND DISPLAYS).

(continued next screen)
Press any key to continue...
```

Screen 6.23

```
5) A list of important COMPUTER SYSTEM components (HARDWARE).

6) A list of all other hardware items necessary for computer operation,
such as air conditioning units, backup power supplies, etc.

7) A list of any additional hardware, equipment, and supplies that might be
needed for smooth functioning of the daily business in order to recover
quickly from a major disaster or catastrophe.


Press any key to continue...
```

Screen 6.24

11. You will be asked to answer some questions that allow LAVA/CS to determine the security level of your data center. After these questions have been answered, LAVA/CS will determine the security level of your data center.

12. Next, you will be asked to select the classification level for the vulnerability reports. Please follow the instructions that appear on the screen.

13. After the classification level for the vulnerability reports has been selected, you will be asked to enter information regarding your organization and those persons participating in the assessment. Please follow the instructions appearing on your computer screen.

```
QUESTIONS ABOUT YOUR ORGANIZATION

After these definitions, explanations, and instructions that you are
receiving, you will be asked today's date and some information about your
organization and all those persons who will participate in this assessment.

THESE QUESTIONS MUST BE ANSWERED. The prompts indicate the spacing
allocated to each answer.  If adequate space has not been allocated, please
abbreviate the information to some form that is easily understandable.  You
will be asked to supply the NAME AND ADDRESS OF YOUR ORGANIZATION and
the SPECIFIC SITE OR LOCATION of the computer installation being assessed.
The address information will include STREET ADDRESS, CITY, COUNTY, STATE,
ONSITE AREA (for facilities that have discrete physical areas), BUILDING
NAME or NUMBER, and ROOM NUMBER(S). There is a separate prompt for each.

In addition to organization information, you will be asked to supply
the name of each person participating in this assessment, their division or
sub-organization within the organization, their title, a brief description
of their responsibility, and their telephone number.  This information will
be used if questions arise during the analysis.  WHEN THE INFORMATION HAS
BEEN ENTERED FOR THE LAST PARTICIPANT, respond with a <RETURN> or <ENTER>
key when prompted for the next name.
Press any key to continue...
```

Screen 6.25

```
Date-------------------

Facility/Organization--

Computer Installation--

Street address---------

City-------------------

County-----------------

State------------------

Zip Code---------------

Onsite Area------------

Building---------------

Room(s)----------------
IF THESE ENTRIES ARE CORRECT -- PRESS <RETURN> or <SPACEBAR>
IF INCORRECT -- PRESS ANY OTHER CHARACTER
```

Screen 6.26

```
For each person participating in answering this questionnaire
list the following information:

Name-(press <RETURN> when done)---

Department --

Title --

Responsibility --


Mail code --

Phone no.  --



IF THESE ENTRIES ARE CORRECT ..  PRESS <RETURN> or <SPACEBAR>
IF INCORRECT ..  PRESS ANY OTHER CHARACTER
```

Screen 6.27

14. LAVA/CS next will prepare you to begin answering the questionnaire. Please pay close attention to the input conventions appearing on the screen. General information regarding the categories of questions in the questionnaire is presented.

```
ANSWERING THE VULNERABILITY QUESTIONNAIRE


The vulnerability questionnaire is administered by the programs on
the QUESTIONS diskette.

The questions for analyzing your computer security vulnerability will
begin.  As each question appears on the screen, you will be prompted
for an answer.  LAVA/CS will store your answers for the vulnerability
calculations that LAVA/CS will do when the questionnaire is completed.

Most of the questions can be answered as YES or NO. All questions
of this kind will accept Y, y, T, or t for YES and will also
accept N, n, F, or f for NO.

Occasionally some questions will ask for additional information, or
for a selection of one or more options.  These questions will accept a
brief statement of the answer in the first case, or, in the second case, a
list of the letters of your chosen selections (no delimiters necessary).
When a brief statement is asked for, please respond in TWENTY OR FEWER
CHARACTERS - a longer answer will be truncated after 20 characters.
Press any key to continue...
```

Screen 6.28

```
The questions appearing on the screen are structured LOGICALLY in terms
of safeguards ELEMENTS, their ATTRIBUTES, and additional INFORMATION. Each
question is identified in the upper right-hand corner of the screen by
a question number.  You may note that often these numbers are not in
sequence.  This happens when some questions are skipped because your
answers to previous questions indicate the skipped questions are not
applicable to your circumstances.  You are never asked a question more than
once because of the spatial and logical ordering of the questionnaire.

In addition to the question and its associated number, you will
observe that another item appears on the screen - the general category of
this specific question.  These categories help identify the context
of the current question.  In addition, as the categories change, you have
the opportunity to stop and restart later.  Most categories are about fifty
questions in length, currently ranging from only a few to about 65 questions
per category.  LAVA/CS keeps track of completed categories for you.

The categories you will see are:

Press any key to continue...
```

Screen 6.29

```
                          LAVA/CS Categories

   1.  Area Entry & Authorization          19.  Emergencies & Em.Procedures
   2.  Area Procedure & Policy             20.  Encryption
   3.  Building Construction               21.  Files,Storage Media,Drives
   4.  Building Engineering                22.  General Locale
   5.  Building Entry & Authorization      23.  Heating/Ventilating/Air Conditioning
   6.  Communications                      24.  Housekeeping & Maintenance
   7.  Computer Operating System           25.  Inventory Procedures & Policy
   8.  Computer Operations                 26.  Management Issues & Policy
   9.  Computer Room Construction          27.  Negotiable Financial Documents
  10.  Computer Room Contents              28.  Passwords
  11.  Computer Room Entry                 29.  Perimeter Zone
  12.  Comp.  Room Procedures & Policy     30.  Personnel Privacy
  13.  Computer Room Raised Floor          31.  Storage Media Library
  14.  Computer Room Sensors & Alarms      32.  Terminals
  15.  Computer Room Suspended Ceiling     33.  Transportation
  16.  Data Center Management              34.  Visitors, Vendors, Service Personnel
  17.  Data Traceability                   35.  Stop LAVA now and resume later -
  18.  Emergency & Contingency Plans            (close files for graceful exit)
Press any key to continue...
```

Screen 6.30

```
The purpose for these categories is to provide convenient places to stop
for later restart and to indicate the subjects for similar-appearing ques-
tions (we usually highlight the differences in capital letters).

After you complete each category, the list of categories will appear on
your screen, and you may choose either TO CONTINUE with the questionnaire
OR TO STOP at this point AND RESTART LATER. LAVA/CS helps with the details
of stopping and restarting for you.  Also, this provides a place to make a
backup copy of the answered questionnaire diskette in Drive A:.



Press any key to continue...
```

Screen 6.31

```
NOTE !       NOTE !       NOTE !       NOTE !       NOTE !       NOTE !

     If a question seems inappropriate to you, or if you appear to be asked
about things that do not apply to your computer installation, ANSWER IN
SUCH A WAY THAT THE SAFEGUARD IMPLIED BY THE QUESTION APPEARS TO BE
PRESENT.

     If you think that the safeguard implied by a question is present under
SOME but not ALL circumstances, ANSWER IN SUCH A WAY THAT THE SAFEGUARD IS
PRESENT. The questionnaire is structured so that the subsequent questions
will elicit information about the exceptional circumstances.

     If you are UNSURE about how to answer a question, respond with a '?'
mark which indicates that the implied safeguard appears to be missing.
Make a note of the question number.  When the report is completed, the
safeguard will appear as a vulnerability in the safeguards functions to
which it is related.  At this time, you can determine if it really is a
vulnerability.

Press any key to continue...
```

Screen 6.32

15. The initialization is complete. You are now ready to begin answering the vulnerability questionnaire.

16. Remove the START diskette from drive B.

17. Place the QUESTION diskette in drive B. Proceed to section 6.2 of this tutorial–How to Begin Answering the Interactive Questionnaire–for further instructions.

6.2 How to Begin Answering the Interactive Questionnaire

A complete listing of the questionnaire can be found in Appendix D. We have included in this section copies of the computer screens you will see during the interactive assessment. Because of the size of the questionnaire, we have not reproduced all the screens you will see on your computer screen. We have included information regarding starting the questionnaire and answering the modules, as well as restarting/resuming an assessment.

1. The ANSWER diskette should be in drive A.

2. Users with 2 floppy disk drives should have the QUESTION diskette in drive B.

   NOTE: Hard disk users will need to ensure that they have designated the hard disk as their default drive and are in the LAVA subdirectory.

3. To begin the assessment, type:

   ```
   QUESTION    <CR>
   ```

4. LAVA/CS will present acknowledgments and will ask if you are running the software from a hard disk. Please respond as appropriate.

5. Next, you will be asked if you are restarting the assessment. If you are just beginning the assessment, enter "N". If you have already answered some modules and are restarting the assessment, enter "Y". You will be given an opportunity to double check your input.

6. LAVA/CS next presents each of the 34 modules (or categories) of questions for your selection. The modules are presented in three parts on your computer screen. You may scroll back and forth among the screens by pressing the ENTER key on your keyboard.

```
Mod Module                                        Number of      Answered
 #  Name                                          Questions
 1) Area Entry & Authorization                       30            N
 2) Area Procedure & Policy                          30            N
 3) Building Construction                            33            N
 4) Building Engineering                             33            N
 5) Building Entry & Authorization                   55            N
 6) Communications                                   12            N
 7) Computer Operating System                        25            N
 8) Computer Operations                              20            N
 9) Computer Room Construction                       32            N
10) Computer Room Contents                           33            N
11) Computer Room Entry                              54            N
12) Computer Room Procedures & Policy                43            N
13) Computer Room Raised Floor                       28            N
14) Computer Room Sensors & Alarms                   25            N
15) Computer Room Suspended Ceiling                  14            N
16) Data Center Management                           62            N

    Press:   <ENTER> to display more modules
             ##   to answer a specific module number
             35   to stop, or end of questionnaire
    Enter selection:
```

Screen 6.33

```
Mod Module                                        Number of      Answered
 #  Name                                          Questions
17) Data Traceability                                13            N
18) Emergency & Contingency Planning                 44            N
19) Emergency Situations & Procedures                61            N
20) Encryption                                        3            N
21) Files, Storage Media, & Drives                   21            N
22) General Locale                                   20            N
23) Heating, Ventilation, & Air Conditioning         29            N
24) Housekeeping & Maintenance                       16            N
25) Inventory Procedures & Policy                    11            N
26) Management Issues & Policy                       60            N
27) Negotiable Financial Documents                    8            N
28) Passwords                                        47            N
29) Perimeter Zone                                   62            N
30) Personnel Privacy                                10            N
31) Storage Media Library                            16            N
32) Terminals                                        13            N

    Press:   <ENTER> to display more modules
             ##   to answer a specific module number
             35   to stop, or end of questionnaire
    Enter selection:
```

Screen 6.34

```
Mod Module                                          Number of      Answered
 #  Name                                            Questions
33) Transportation                                      6             N
34) Visitors, Vendors, & Service Personnel             29             N
35) End of questionnaire or stop now                    0             N

     Press:   <ENTER> to display more modules
              ##   to answer a specific module number
              35   to stop, or end of questionnaire
     Enter selection:
```

Screen 6.35

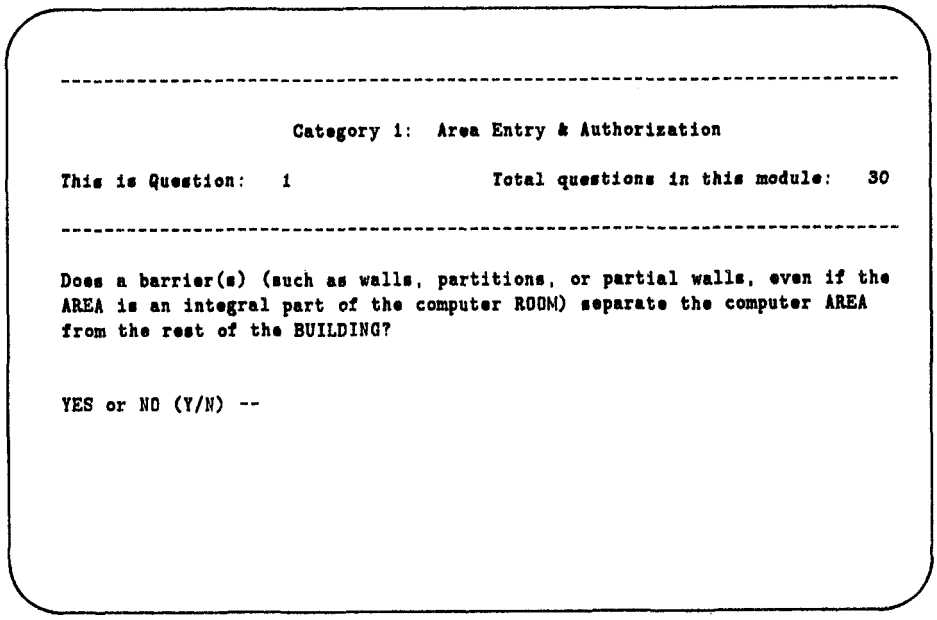
Please note that each screen contains the module number, the name of the module, the number of questions contained in each module, and whether or not the module has been answered. You may select a module by entering the module number. If you have answered all the modules in the questionnaire, or if you are exiting for a future restart, you may exit the questionnaire by entering the number 35.

IMPORTANT: The questions contained in a module must be answered sequentially. You cannot skip backward or forward to answer/re-answer questions within a module. Therefore, it is important that a consensus be reached before a response to any question is entered into the computer. You may, however, re-answer an entire module once it has been answered.

7. You may now select a module. Enter the module number. If you have entered a module number in error, you will be given the opportunity to re-enter your selection.

8. The first question in the category you have selected will be displayed on your computer screen. Note the module heading appearing at the

top of the computer screen. This heading includes the title of the module, the number of questions in the module, and the question number you are answering. You may not be required to answer all questions in each module; the questions you will be asked are determined by the methodology and your responses to previous questions.



Screen 6.36

9. Answer as many modules as you would like.

10. If you wish to exit the questionnaire for a later restart

    (a) Exit by entering the number 35 and a <CR>.

    (b) Remove the diskettes from both drives.

    (c) At this point, you may wish to make a backup copy of the ANSWER diskette to ensure against accidental loss of data. If you have a computer system with two floppy disk drives, follow the instructions listed below. If your computer system has one disk drive, please consult your DOS manual for disk copying instructions.

        i. Place the ANSWER diskette in drive A.

ii. Place a blank, formatted diskette into drive B.

iii. Type:

```
A: copy*.* B:      <CR>
```

iv. Remove the diskettes from both disk drives.

11. Turn off your computer.

12. When you are ready to resume, start up the computer with `CONFIG.sys` file on the system diskette.

13. Make sure the ANSWER diskette is in drive A and the QUESTION diskette is in drive B. Change the default drive to drive B by typing:

```
B:          <CR>
```

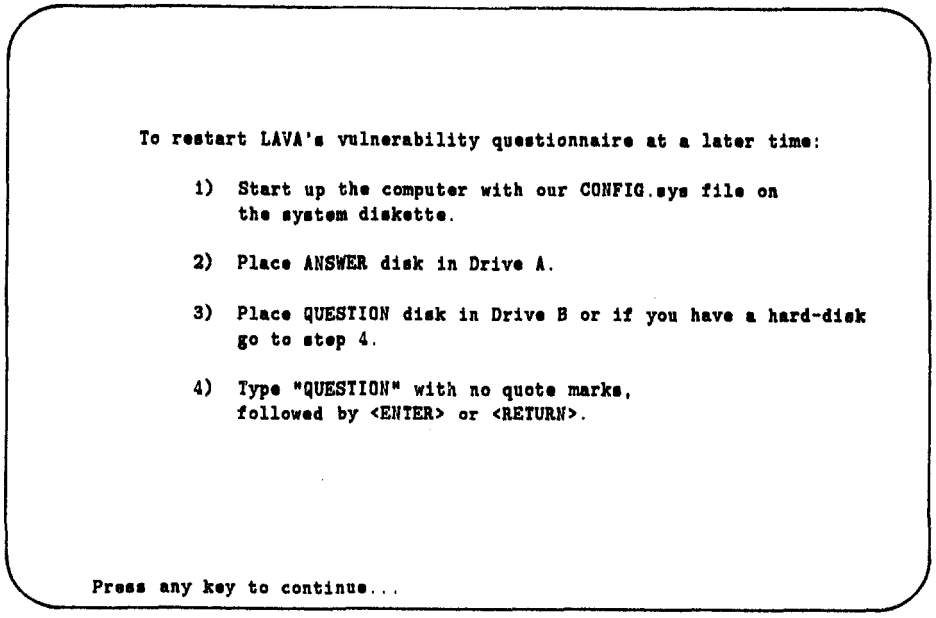
14. If you have a computer system with two disk drives, place the QUESTION diskette in drive B, and change the default drive to drive B by typing:

```
B:      <CR>
```

    If you have a system with a hard/fixed disk, make sure you are logged on to the default drive (C:) and in the LAVA subdirectory.

15. Type:

```
QUESTION
```



Screen 6.37

TO STOP FOR A SHORT BREAK: If you wish to stop for a few minutes, you need not follow the above instructions. Instead:

(a) Exit by entering module number 35 and a <CR>,

(b) Leave the ANSWER diskette in drive A and leave the QUESTION diskette in drive B and

(c) Restart the questionnaire by typing QUESTION <CR>.

16. Because the ANSWER diskette contains all of your responses to the questionnaire, we urge you to make a back-up copy of the ANSWER diskette each time you exit the QUESTION diskette for a later restart (and at frequent intervals throughout the assessment period) to ensure against accidental loss of data (see instruction 10c above).

17. You may begin the scoring by placing the diskette labelled SCORE into drive B. Proceed with instructions given in section 7.1 of the Tutorial—Scoring the Questionnaire.

Chapter 7

SCORING THE QUESTIONNAIRE

7.1 Scoring the Questionnaire

Scoring the questionnaire takes approximately 1 to 1 1/2 hours to complete and may be initiated once all modules have been answered. If you would like to terminate the scoring process once it has been initiated, type ALT C. Please note that any data generated by the scoring program prior to termination of this type will not be saved for a later restart; you will have to begin the scoring process again.

1. The ANSWER diskette should be in drive A.
2. The SCORE diskette should be in drive B.
3. If your computer has two floppy disk drives, change the default drive to drive B by typing

   ```
   B:      <CR>
   ```

   NOTE: Hard/fixed disk users will need to ensure that they have designated the hard/fixed disk as their default drive and that they are in the LAVA subdirectory.
4. To begin the scoring process, type:

   ```
   SCORE     <CR>
   ```

6. Next, the vulnerability scores will be calculated. The program will keep you apprised of its progress. Please note that the scoring process will take 1 to 1 1/2 hours to complete.

```
      INITIALIZING VULNERABILITY MATRIX

      DETERMINING REACHABILITY MATRIX

      CALCULATING VULBERABILITY SCORES, TOTALS AND MESSAGES

            Working on question number 998

      STORING THE VULNERABILITIES/TOTAL APPLICABLE QUESTIONS

            Event tree 21 Branch number 2

      RANKING THE VULNERABILITIES

      PREPARING RANKED INFORMATION FOR REPORT GENERATOR


SCORING CALCULATIONS ARE NOW COMPLETE

Press any key to continue...
```

Screen 7.1

7. Once the scoring has been completed, you will be ready to print the vulnerability reports. Place the REPORT diskette into drive B. Proceed with section 8.1 of the Tutorial—Printing the Vulnerability Reports.

Chapter 8

PRINTING THE REPORT

8.1 Printing the Vulnerability Report

Examples of the LAVA/CS Vulnerability Reports may be found in the appendix. The reports will take a couple of hours to print. Please make sure you have at least 250 pages of fan-fold paper for your printer before you begin.

1. Your printer should be turned on and should be connected to the computer.

2. Make sure you have sufficient paper on which to print the reports.

3. Place the ANSWER diskette in drive A, and place the REPORT diskette in drive B.

4. If your computer system has two floppy disk drives, change the default drive to drive B by typing

   ```
   B:      <CR>
   ```

   NOTE: Hard/fixed disk users will need to ensure that they have designated the hard/fixed disk as their default drive and that they are in the LAVA subdirectory.

5. There are two ways to print the reports. You may begin printing the reports immediately after the scoring has been completed, or you may complete the scoring and print the reports at a later time.

To begin the printing immediately after the scoring has been completed, type

```
REPORT      <CR>
```

and follow the directions appearing on the computer screen.

6. To print the reports after the scoring has been completed:

   (a) Turn on the computer.

   (b) If your computer system has two disk drives, change the default drive to drive B by typing

   ```
   B:      <CR>
   ```

   If your computer system has a hard disk, make sure you are logged on to the default drive and into the LAVA subdirectory.

   (c) To begin printing the reports, type

   ```
   REPORT      <CR>
   ```

7. Follow the instructions as they appear on your computer screen.

   NOTE: A response to "Press any key to continue" for will result in an immediate paper advance and printing will begin.

   The first two pages to be printed are the first and last pages of the report.

Appendix A

DOE REGULATORY BASIS FOR LAVA

Office of Management and Budget
OMB Circular No. A-71 March 6, 1965
supplemented by Transmittal Memorandum
No. 1 "Security of Federal Automated
Information Systems" July 27, 1978

Established policy and responsibilities for the development and implementation of computer security programs. Assigned responsibility for the conduct of periodic risk analyses. Requires a measure of relative vulnerabilities.

Office of Management and Budget
OMB circular No. A-123 October 28, 1981
"Internal Control Systems" Revised: August 16, 1985

Established internal control standards and a system of agency responsibilities and requirements. Provided for an on-going program of vulnerability assessments at least every 2 years. Concerns all agency components and assessable units.

Department of Energy
DOE Order 1360.2 March 9, 1979
"Computer Security Program for Unclassified Computer Systems"

Established policies and procedures for developing, implementing, and administering a program for safeguarding DOE computer systems. Requires periodic risk analyses performed in less than 5 year intervals.

Department of Energy
DOE Orders 5636.2 and 5636.4 January 10, 1980
"Security Requirements for Classified Data Processing Systems"

Established uniform requirements, policies, and responsibilities for the development of a program to ensure the security of information stores in classified ADP systems.

Department of Energy
Order 1000.3 and April 23, 1982
Order 1000.3A August 30, 1985

Require vulnerability assessments to be conducted at an aggregate level at least biannually using a team approach.

Appendix B

LAVA Glossary

ADP - Acronym for Administrative Data Processing or Automatic Data Processing.

Access Controls - Techniques restricting access to a physical area or to a computer so that only authorized users are allowed.

Accountability - The property that enables violations or attempted violations of system security to be traced to individuals who may then be held responsible.

Acoustic Coupler - A device for coupling electrical data lines to acoustic telephones for data transmission through the telephone system.

Algorithm - A specified series of steps for accomplishing a prescribed function.

Applications - Those portions of a system, including portions of the operating system, that are not responsible for enforcing the system's security policy.

Applications Programmer - Responsible for designing, developing, testing, documenting, and maintaining programs for user applications.

Applications Software - Programs designed by users to accomplish specific tasks for those users.

Area - Comprises locations where computer-related activities take place and where information considered by the organization to be worthy of

protection is held, used, processed, or stored; not necessarily contiguous to the computer room(s).

Asset - An item or collection of items that have tangible or intangible value to the subject organization.

Audit - Independent review and examination of records.

Audit Trail - A set of chronological records allowing reconstruction of events.

Authenticate - To establish the validity of a claimed identity.

Automatic Disconnects - A switching system that can be applied to telephone circuits so that the circuit is disconnected some distance from the telephone. Prevents unintended energy from equipment near the telephone from being coupled onto telephone circuits.

BCF - Bromochlorodifluoromethane; $CBrClF_2$; also known as Halon 1211. BCF is a gas used for fire suppression.

BPS - Acronym for "bits per second."

BUS - A connection medium to which multiple nodes may be connected. The nodes are essentially independent from other node connections, but can communicate with the other nodes.

Back-up - A method of ensuring maintenance of essential capabilities if crucial facilities or data are lost.

Barrier - An object that separates or is used as a barricade. As used in LAVA, barrier applies to the enclosing media and not to any penetrations through the enclosing media.

Baseband - A local area network communication technique where the data are entered directly onto the transmission medium with no frequency conversion.

Batch - Large volume data transmission or non-interactive sequences of program execution.

Batch Processing - A computer system designed to handle large volume data transmission or non-interactive sequences of program execution.

Baud - Channel symbols-per-second communication rate. This rate may be lower than the actual flow rate of information.

Bit - A binary digit (either zero or one).

Blackout - A complete loss of power.

Boot - To insert the software into a computer system that will control its operation.

Bootstrap Loader - A loader that inserts itself into memory after a key instruction or instructions (called a "bootstrap") has been inserted or read out of ROM.

Broadband - A local network technique for translating data to relatively high modulated frequency so that the link can be shared by multiple communications.

Brownout - Power reduction due to excessive load.

Buffer - Temporary storage for data that allows insertion and removal under separate synchronization control.

Building - The specific structure(s) housing the computer installation being assessed. Includes all buildings that house information-related activities described in the following definitions of area, computer room, and computer system.

Bypass - Allowing plaintext information to pass around an encryption device without any coding.

Byte - A group (usually 8) of binary digits (bits).

CCERP - Computer Center Emergency Response Plan

CPU - Central processing unit; sequential logic circuitry containing arithmetic logic units, instruction decoding circuitry, time, and control circuits, temporary storage registers and program counters.

CRT - Cathode Ray Tube (a common display device).

Cable - Stranded assembly of electrical conductors twisted around a central core, usually heavily insulated by outside wrappings.

Cache - High-speed memory used as a buffer between main memory and the CPU.

Central Computer Facility - A powerful, centralized computing capability that multiple users can share.

Channel - An information transfer path within a system. May also refer to the mechanism by which the path is effected.

Chip - A small piece of semiconductor substrate usually containing an integrated circuit.

Ciphertext - Text that has been encoded to protect the information from unauthorized observation.

Circuit - A communications link between two or more points.

Circuit Breaker - Magnetic or electro-mechanical device that self-interrupts when power demands become excessive.

Class A Fire - A fire of ordinary combustibles, such as paper, wood, cloth or plastics.

Class B Fire - A flammable liquid and vapor fire.

Class C Fire - Fires involving electrical energy.

Classified Data - Data requiring protection against unauthorized disclosure in the interest of national security.

Classified Information - Information or material that is owned by or under the control of the U.S. Government, determined under Order 12356 or prior orders to require protection against unauthorized disclosure.

Cleartext - Ordinary text as it would be transmitted uncoded.

Clock - A signal occurring at regular intervals from which to derive system timing.

Code - Depending on the context, either a digital representation of numbers, letters, or symbols; or a program.

Coding - A method for representing information in a different form.

Cold Site - A back-up or recovery facility into which computers can be moved by members of an organization in case of a disaster.

Common Cause Analysis - An analysis in which vulnerability and loss exposures that occur in a variety of ways from a multiplicity of causes are identified.

Communications Engineer - A staff member who works with the communications equipment that convey computer data. Such equipment might include wiring, modems, encryption equipment, diagnostic and monitoring equipment.

Communications Link - The physical means of connecting one location to another for the purpose of transmitting and/or receiving data.

Communications Security - Protective measures taken to deny unauthorized persons from obtaining information derived from telecommunications of the U.S. Government related to national security and to ensure the authenticity of such communications.

Compromise - A violation of the security system such that an unauthorized disclosure, modification, or destruction of sensitive information may have occurred.

Computer - A relatively high-speed device containing a CPU to execute instructions, memory, I/O, and software.

Computer Abuse - The misuse, destruction, alteration, or disruption of data processing resources for reasons other than monetary gain.

Computer Operator - Person(s) in control of basic computer operations, usually from a console.

Computer Room - A partitioned space housing the data-processing and related equipment. May include media vaults, telecommunications closets, office space for system support personnel, maintenance workshops, and storage space for related supplies.

Computer Security Specialist - Person responsible for planning, implementing, installing, operating and evaluating security safeguards and controls.

Computer System - Encompasses both the computer-related machinery and the storage media upon which information (programs, data, results) is stored in non-human-readable form.

Computer Systems Engineer - Person responsible for system hardware (CPU and peripherals), including test, diagnosis and repair.

Concentrator - Also known as "multiplexer"; a device that connects several input lines sequentially to a single output line so that the output carries interspersed data from several sources.

Confidential - Information requiring protection from unauthorized disclosure.

Consequences - The results of a consequence analysis for which outcome and impact measures are combined to produce a measure of consequences.

Contingency Plan - Procedures for emergency response, back-up and recovery in the event of a disaster.

Contingency Planning - A program to minimize the potential disruption of computing capabilities in the event of a disaster.

Controlled Access - Access into a facility, building, perimeter, area, or room which is either locked, has intrusion devices mounted, or has guards posted to control admission into the area.

Controller - A dedicated processor that controls some activity or process that cannot be used for general purposes.

Core - A small magnetic toroid used in computer memories.

Data - A representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by human or by automatic means.

Data Center - The location at which all computer-related and information-related activities are performed. These activities include input preparation, output distribution, computer operations, report documentation and distribution, and media library storage.

Data Integrity - The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction.

Dedicated Security Mode - The mode of operation in which the system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information for which all users have the appropriate clearance and need-to-know.

Degauss - To demagnetize magnetic media by applying a reverse magnetizing force.

Degausser - Equipment used to demagnetize ADP magnetic storage media.

Dial-Up - The service whereby a telephone can be used to initiate and effect communication with a computer. Dial-ups present potential security hazards.

Directory - Descriptive information pertaining to files and file-access controls.

Discretionary Access Control - A means of restricting access to objects based on the identity of subjects and/or groups to which they belong.

Disk - Magnetic recording device for mass storage using a flat, circular recording medium.

Diskette - A thin, circular, flexible sheet of Mylar with a magnetic-oxide surface on which data can be recorded in tracks and from which data can be read. Sometimes called a floppy disk.

Distributed Processing - A system including linked CPU's in which processing takes place in more than one CPU.

Distributed Systems - Systems whose components are not centrally located and are connected by communications media.

Download - The transfer of data or programs from one computer to another; typically from a mainframe to a microcomputer.

EDP Auditor - A person who performs an independent security analysis and performance check of computer systems by reviewing and testing performance and security features.

Emergency Response - Immediate action taken in the event of a disaster to limit overall effects and computing impact.

Encryption - A method of applying a cryptographic key to plain text to encipher or encrypt.

Erasure - A method by which a signal recorded on magnetic media is removed. Erasure is accomplished in two ways: alternating current erasure and direct current erasure.

Expired Password - A password that must be changed by the user before login may be completed.

Exterior Windows - Windows contained in the outer walls of a structure.

Facility - The physical and procedural environment of the parent organization of one or several information processing center(s). It is not restricted only to buildings in which the actual information processing takes place.

Faraday Shield - A screen or cage of wires intended to protect against the transmission of electrostatic energy.

File Protection Ring - A detachable ring used in conjunction with a tape drive unit to protect data on a magnetic tape.

File Security - The means by which access to computer files is limited to approved operators only.

Fire Walls - Walls that have been sufficiently fireproofed to prevent the spread of fire.

Firmware - A piece of hardware (e.g., a ROM) that implements a software routine.

Floppy Disk - Low-cost mass storage medium on which data can be recorded in tracks and from which data can be read. Sometimes called a diskette.

Formal Verification - The process of using formal proofs to demonstrate the consistency (design verification) between the formal specification of a system and its program specification.

Functional Testing - The portion of security testing in which the advertised features of a system are tested for correct operation.

General-Purpose System - A computer system that is designed to aid in solving a wide variety of problems.

Generic Outcome - Generic outcomes can include such things as unauthorized access or use, denial of use, damage or destruction, noncompliance with applicable laws or regulations, waste, misappropriation, disclosure, theft and modification or tampering.

Granularity - The size of the smallest protectable unit of information.

Group Access - Common (shared) file access for a group of users.

HVAC - Heating, ventilation and air conditioning.

Halogen - A chemical series including fluorine, chlorine, bromine and iodine.

Halon System - A fire suppression system using Halon gas. Halon is especially suited for computer facilities because it does not damage electronic equipment.

Handshaking - An interchange of signals between two devices that must communicate to prepare for or terminate a connection or data transfer.

Hardware - The electric, electronic, and mechanical equipment used for processing data. Hardware may consist of cabinets, racks, tubes, transistors, wires, motors, and such.

Harm - An adverse condition in an asset resulting from an action by a threat; examples of such adverse conditions might include damage or destruction, unauthorized access or use, loss, or tampering. (See Outcome).

Hierarchical Decomposition - The ordered, structured reduction of a component to its most elementary security property.

Host - A computer that accepts and processes jobs from remote terminals or computers.

Hot Site - A backup or recovery computer facility that can be temporarily used by members in case of a disaster.

Impact - The monetary and non-monetary costs or losses associated with a particular outcome for a specific threat-asset pair interaction exploiting a vulnerability in a specific safeguards function.

Intelligent Terminal - A data communications terminal with data storage and processing capabilities.

Interactive - Real-time dialogue between terminal and computer.

Interior Windows - Windows contained in the interior walls of a specific structure.

Key - 1. Physical entity to unlock and sometimes lock a lock; 2. an electronic signal or data patterns to allow the logical operation desired; 3. a combination of characters, numbers of both to be examined prior to granting access to an area, computer, or file.

Key Generator - A device for encrypting-key generating.

LAN - Acronym for "Local Area Network". Interconnection and communication mechanisms for office and computer-data traffic that allows common access to a communication medium. The distance usually spanned is a mile or less.

Least Privilege - This principle requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks.

Library - A collection of software programs or routines.

Link - A connection (not necessarily hardwired) for communications.

Loader - Software program for loading a program into memory.

Logic Bombs - Unauthorized, malicious destructive routines that are initiated by some parameter such as time and date.

Magnetic Remanence - A measure of the magnetic flux density remaining after removal of the applied magnetic force. Refers to any data remaining on ADP storage media after removal of the power.

Mainframe Computers - Large central-site computers that provide state-of-the-art computing capabilities.

Malicious Logic - Hardware, software or firmware that is intentionally included in a system for the purpose of causing loss or harm (e.g., Trojan Horse).

Mandatory Access Control - A means of restricting access to objects based on the sensitivity of the information contained in the objects and the formal authorization of subjects to access information of such sensitivity.

Masquerading - Attempting to gain access to a computer system by posing as an authorized user.

Memory - Computer accessible storage area for information and data.

Microcomputer - A small computer based on a microprocessor and intended for individual use.

Microprocessor - A small device usually built on a small semiconductor chip that has rudimentary computer capabilities such as instruction processing, logic, arithmetic, and control.

Minicomputer - A small (usually desk size) computer with relatively limited capabilities, compared to mainframes.

Modem - Modulator-demodulator. A device that receives digital data and conveys the information by modulating a carrier for transmission over communications media.

Monetary - An impact measure in terms of dollars. Used for those outcomes whose impact can be measured in dollars, such as the cost of fraud or embezzlement.

Multilevel Device - A device that is used in a manner that permits it to simultaneously process data of two or more security levels without risk of compromise.

Multilevel Network Subject - A network subject that causes information to flow through the network at two or more security levels without risk of compromise.

Multilevel Secure - A system containing information with different security classifications that simultaneously permits access by users with different security clearances and need-to-know. Prevents users from accessing information for which they lack authorization.

Multiplexing - Interleaving or simultaneously transmitting two or more messages on a single channel.

NBS - National Bureau of Standards

Networks - Associated components interconnected for such functions as communications and resource sharing.

Node - A network termination point (computer, terminal, switch).

Non-Monetary - An impact measure given as a linguistic description (such as nuisance, acceptable, catastrophic). Used for those outcomes for which monetary measures do not make sense, such as for loss of reputation or for the "cost" of organizational embarrassment.

Nonvolatile Memory - Memory that is retained when power is shut off.

Object - A passive entity that contains or receives information. Access to an object potentially implies access to the information it contains. Examples are: records, blocks, pages, files, directories and programs, video displays, keyboards, clocks, and printers.

Object Code - The representation of a program after translation from source code to a form directly executable by a computer.

Object Creation - A special type of access that theoretically must be performed upon an object before any read, write, or other access to that object is permitted.

Off-Site Storage - A storage site located outside the zone of the natural hazard being guarded against. For example, if the facility is located in a flood plain along a river, the off-site storage should not be located in the same flood plain.

Operating System - An integrated collection of service routines for supervising the sequencing and processing of programs by a computer. Operating systems control the allocation of resources to users and their programs.

Outcome - The result of a threat exploiting a vulnerability in a safeguards function for a particular asset. Outcomes can have varying degrees of outcome severity.

Output - Information that has been exported by a trusted computing base.

Output Spy - A program that allows one to see what is being printed on someone else's terminal.

Parity - A measure of the number of ones in a sequence; either odd or even.

Passphrase - A phrase used in the same manner as a password to control user access.

Password - A private character string used to authenticate and identify. Knowledge of the password is considered proof of authorization to access a system.

Password System - A part of an ADP system that is used to authenticate a user's identity. Assurance of unequivocal identification is based on the user's ability to enter a private password that no one else should know.

Penetration - The successful, repeatable, unauthorized extraction of recognizable information from a protected data file or data set.

Perimeter Zone - The organizations's grounds and buildings which may or may not be fenced. The area logically associated with the individual site for which the assessment is being performed.

Personal Computers - Computers originally intended for use in the home by hobbyists or for operations not related to business. These are now used commonly as small business computers.

Piggybacking - Gaining unauthorized access to an ADP system via another user's legitimate connection.

Piracy - Unauthorized copying of software or hardware usually for financial gain.

Polling - Sequential sampling or reading information that has been stored awaiting a query.

Port - A connection through which information can pass interfacing one system with another.

Power Line Disturbance Analyzer - An instrument for identifying and characterizing various power problems.

Privacy - Right (legal or social) of an individual to control collection, storage and dissemination of personal information.

Process - A program in execution. It is completely characterized by a single current execution point and address space.

Processor - A device for interpreting and acting on program inputs.

Programmed - 1. controlled by software; 2. controlled by hardware or firmware implementation of software.

Programming - Depending on the context, programming has various meanings including writing a sequence of instructions; physically inserting data into ROM or PROM; setting up an address by electrical connections to which particular devices will respond.

Protocol - Rules, procedures, or format for presenting information sequentially.

RAM - Random Access Memory; a read-write memory that data can be written into as well as read from.

ROM - Read Only Memory; memory from which data can be obtained and in which the data are permanently fixed according to specifications.

Raised Floor - Any floor which is above another surface (e.g., a standard computer floor installed on top of the load bearing floor). The distance between a raised floor and the surface below it may be as little as the thickness of a 2x4 or as much as a basement.

Random Access - Memory access to a specified location without waiting to arrive at the data or data location sequentially.

Read - Process of examining data in memory by deriving signals that directly represent the data. Reading is usually a nondestructive process. That is, the data are unaltered in memory after the read process.

Read Access - Permission to read information.

Recovery - Restoration of computing facilities and capabilities.

Red/Black Concept - Separation and routing control to prevent inadvertent coupling between red (carrying classified) and black (not protected for classified) wiring.

Register - Storage device for temporarily storing a group of associated bits.

Releases - Supported modifications made to languages, operating systems, and other software.

Remote Terminal - A terminal located away from the central site.

Removable Storage Media - Tapes, disk packs, or floppy diskettes that can be easily removed from the system.

Resource - Anything utilized or consumed while performing a task. The categories of resources are: time, information, objects, or processors.

Risk - The exposure to loss, arrived at by combining the outcome severity measure with the monetary and non-monetary impact measures .

Risk Analysis - A technique for quantifying the value of statistically expected losses resulting from vulnerabilities and for quantifying the cost per unit of time of techniques for combating vulnerabilities. Aids in evaluating the desirability of security measures .

Risk Assessment - A systematic evaluation of the potential losses that the subject organization might suffer if vulnerabilities are exploited.

SSO - Acronym for "system security officer." The person responsible for the security of an ADP system.

Safeguards - A collection of policies, procedures and countermeasures that protect an asset from a threat.

Safeguards Function - A major function required to protect a specific asset from the actions of a specific threat. Each threat-asset pair can interact only in certain ways, and a specific set of safeguards functions combine together to achieve complete protection.

Salami Technique - The process of removing small slices of assets so that removal is unnoticed but aggregate over time is substantial.

Sanitizing - Erasing or overwriting information so it will not be inadvertently disclosed.

Scavenging - Physical or electronic search for remnant data that may have not been properly destroyed; such as reading assigned file space prior to writing into the space.

Secure Front End - A security filter, which could be implemented in hardware or software, that is logically separated from the remainder of the system to protect its integrity.

Security - Protection from harm, such as unintended disclosure, alteration, destruction, misuse or vandalism.

Security Kernel - Central hardware or software that performs security functions.

Security Level - The combination of a hierarchical classification and a set of nonhierarchical categories that represents the sensitivity of information.

Security Policy - The set of laws, rules and practices that regulate how an organization manages, protects and distributes sensitive information.

Sensitive Information - Information that, as determined by a competent authority, must be protected because its unauthorized disclosure, alteration, loss, or destruction will at least cause perceivable damage to someone or something.

Separation of Duties - The concept of dichotomizing at least some of the functions of authorizing, approving, recording, issuing, paying, reviewing, auditing, programming, and developing operating systems among separate personnel.

Shell - A backup or recovery facility (a cold site) into which computers can be moved in case of a disaster.

Smoke Detector - A device that senses particles of combustion.

Software - Programs of instructions, including the operating programs and programs for editing, program conversion, and loading data into memory.

Source Code - The representation of a program as written by a programmer or as otherwise entered into the initial computer processing.

Standalone - A system that functions independently of other systems.

Storage Object - An object that supports both read and write accesses.

Subject - An active entity, generally in the form of a person, process, or device that causes information to flow among objects or changes the system state. Technically, a process/domain pair.

Superminicomputers - Advances minicomputers with many of the capabilities formerly found only in mainframes.

System - An assembly of computer hardware, software, and firmware configured for the purpose of classifying, sorting, calculating, computing, summarizing, transmitting and receiving, storing and retrieving data with a minimum of human interaction.

System Users - Those individuals with direct connections to the system and also those individuals without direct connections who receive output or generate input.

Systems Programmer - Software developer responsible for the design, development, installation, and documentation of the operating system, peripheral utility programs and modifications.

Systems Software - Programs that extend system capabilities.

Tape Librarian - Person in charge of filing, retrieving, and accounting for storage media (tapes, disk packs, cartridges).

Technical Vulnerability - A hardware, firmware, or software flaw that leaves a computer processing system open for potential exploitation either externally or internally.

Telecommunications - Communication over relatively large (usually more than a few hundred meters) distances, usually by microwave, but sometimes over hardwired lines.

Tempest - A term commonly used to describe the emanation of information by unintended means such as electromagnetic, electrical, and acoustic propagation so that it might be intercepted by unauthorized personnel.

Terminal - A data-entry device for communicating alphanumeric characters, programs, and commands to computers and similar devices. They may or may not have "intelligence" (the ability to store, modify, or edit data before transmission).

Threat - An active natural or random hazard, such as fire, flood, power outage, earthquake, volcanic eruption, random human error, or an intentional human action that causes some form of harm to an asset.

Threat Analysis - The examination of all actions and events that might adversely affect an ADP system, facility or operation. Looking at all potentials for damage.

Threat-Asset Pairs - All possible combinations of threats and assets taken two at a time.

Transparent - Internal actions that are not obvious to external users.

Trap Doors - 1. Breaks in programs to allow for insertion of steps and to provide intermediate output for diagnosis, and 2. cryptographic techniques for solving a computationally difficult problem by using additional crucial information.

Trojan Horse - Covert unauthorized instruction sequence within an authorized program.

Trunks - Shared communication links between nodes or switches.

Trusted - A component is said to be trusted if it can be relied on to enforce the relevant security policy.

Uninterruptible Power Supply (UPS) - A system that can maintain AC power during a temporary outage by continuing to derive DC power from batteries and convert to AC power in the event that commercial power becomes unavailable or is outside normal limits.

User - Any person who interacts directly with a computer system.

User ID - A unique symbol or character string that is used by an ADP to uniquely identify a user.

User Programmer - A person who designs, develops, tests, documents, and maintains programs in accordance with user-determined specifications.

User-friendly - A system or program that is easy for users to learn; usually developed for nonprofessionals.

Verification - A weakness in ADP system security procedures, administrative controls, internal controls, etc., which could be exploited to gain unauthorized access to classified or sensitive information.

Vulnerability - A weakness or flaw in a safeguards function, such as in a security system or procedural system, which can be exploited by a threat to cause harm to an asset.

Vulnerability Assessment - A systematic evaluation of the vulnerabilities in a safeguards system, broken down by safeguards functions. Ideally, it will include a complete list of all the exploitable weaknesses for each safeguards functions.

Wiretapping - Passive monitoring of communication channel(s) surreptitiously.

Write - The process of inserting data into memory. This process is destructive in that any data already in a particular memory location are destroyed when new data are written into that location.

Write Access - Permission to write an object.

Write Ring - A ring that can be inserted into a reel of magnetic tape that enables the tape-deck writing process. Removal of the write ring prevents writing.

Appendix C

Background Papers

LA-UR -85-1933

Los Alamos National Laboratory is operated by the University of California for the United States Department of Energy under contract W-740

TITLE: FRAMEWORK FOR GENERATING EXPERT SYSTEMS TO PERFORM COMPUTER SECURITY RISK ANALYSIS

AUTHOR(S): S. T. Smith and J. J. Lim

SUBMITTED TO: First Annual Armed Forces Communications and Electronics Association Symposium and Exposition on Physical and Electronics Security, Philadelphia, August 19-21, 1985

By acceptance of this article, the publisher recognizes that the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes.

The Los Alamos National Laboratory requests that the publisher identify this article as work performed under the auspices of the U.S. Departm

Los Alamos Los Alamos National Laborat
Los Alamos, New Mexico 87

FORM NO. 836 R4
ST. NO. 2629 5/81

Framework for generating expert systems to perform computer security risk analysis*

S. T. Smith and J. J. Lim**

Los Alamos National Laboratory, Safeguards Systems Group
PO Box 1663, MS-E541, Los Alamos, New Mexico 87545

ABSTRACT

At Los Alamos we are developing a framework to generate knowledge-based expert systems for performing automated risk analyses upon a subject system. The expert system is a computer program that models experts' knowledge about a topic, including facts, assumptions, insights, and decision rationale. The subject system, defined as the collection of information, procedures, devices, and real property upon which the risk analysis is to be performed, is a member of the class of systems that have three identifying characteristics: a set of desirable assets (or targets), a set of adversaries (or threats) desiring to obtain or to do harm to the assets, and a set of protective mechanisms to safeguard the assets from the adversaries. Risk analysis evaluates both the vulnerability to and the impact of successful threats against the targets by determining the overall effectiveness of the subject system safeguards, identifying vulnerabilities in that set of safeguards, and determining cost-effective improvements to the safeguards.

As a testbed, we evaluate the inherent vulnerabilities and risks in a system of computer security safeguards. The method considers safeguards protecting four generic targets (physical plant of the computer installation, its hardware, its software, and its documents and displays) against three generic threats (natural hazards, direct human actions requiring the presence of the adversary, and indirect human actions wherein the adversary is not on the premises--perhaps using such access tools as wiretaps, dialup lines, and so forth). Our automated procedure to assess the effectiveness of computer security safeguards differs from traditional risk analysis methods. The safeguards system is modeled as an interactive conversational questionnaire that elicits information about the presence and quality of system safeguards; it is fully automated in natural language on a portable microcomputer. At the functional level, a set of event trees links the questionnaire with the risk analysis--each safeguards issue pertains to one or more risk functions, such as fire damage prevention or software access controls; the vulnerabilities in the safeguards system are evaluated in light of the risk functions. An assessment is made of the safeguards vulnerabilities using a linguistic scoring method that takes into account the sensitivity of the information processed at the computer installation. Specific pieces of equipment, software, and documents can be specified by the user for a more detailed assessment, and linguistic worths are placed upon these items. Qualitative impact measures are determined for a spectrum of outcome scenarios. The vulnerability worths and impact measures are then combined using a probabilistic linguistic algebra to provide a set of useful, functional risk measures.

The automated vulnerability assessment portion of this methodology is currently in use at the United States Nuclear Regulatory Commission, and is under consideration by the Air Force Computer Security Project Office. It has been tested at selected Department of Energy installations all over the country as well as at the Federal Bureau of Investigation. The methodology is also being used by the Institute for Computer Security and Technology of the National Bureau of Standards and is being considered for further development funding by several other government agencies.

INTRODUCTION

A typical laboratory, organization, or production plant (whatever is defined as the subject system for the analysis) is exposed to numerous significant potential threats and has many assets that can be affected by these threats. The potential risk of the subject system is a function of

*Lim and Orzechowski Associates, Walnut Creek, California.

**Supported by the U.S. Department of Energy, Office of Safeguards and Security, and the U.S. Nuclear Regulatory Commission, Office of Data Automation.

the frequency of the threat occurrence, the loss potential of a given asset, and the system vulnerabilities that provide the link between the threat and the asset. Risk assessment evaluates both the vulnerability to and the impact of threats achieving their purpose against targets; Fig. 1 depicts this relationship. A risk assessment has three basic objectives: to determine the overall effectiveness of the safeguards protecting the subject system, to identify the vulnerabilities in the safeguards, and to aid in determining cost-effective improvements to the safeguards, if needed.[1,2]

Before our methodology was developed, simple risk analysis tools did not exist. Existing methods either were extremely complicated and labor-intensive, or they existed in the form of unintegrated questionnaires, requiring a great deal of manual manipulation to arrive at any functional information. These methods were resented by the user because of the time required to estimate (or guess at) frequencies, probabilities, and consequences of events. They were resented by management because they usually required the (often costly, often unsecure) services of outside consultants as well as a large amount of time from the user organization's staff. They were frustrating to the analyst because often the resentful user gave inaccurate or incomplete data, resulting in the propagation of errors that could produce erroneous or misleading conclusions.

Often the results from such risk analyses were difficult to use for several reasons. They consisted of unintuitive quantitative measures like annual loss expectancy, they provided little insight about how to enhance system security, and they did not help determine whether the existing level of safeguards is adequate. What really is needed is an affordable, reusable evaluation tool to analyze vulnerabilities and impacts leading to risk. Such a tool, with rigorous theoretical treatment of the subject, would provide both defensible analysis and useful results.

To satisfy the need for a simple, inexpensive, effective method for risk assessment, we are developing at Los Alamos National Laboratory an original methodology that provides the framework for a fully automated, interactive knowledge-based expert system[3] to guide and facilitate the performance of risk analysis on the class of subject systems that can be characterized by a definable set of safeguards protecting a generic set of assets (or targets) from a generic set of adversaries (or threats). The subject system comprises the collection of information, procedures, devices, products, and real property upon which the risk analysis is to be performed.

At Los Alamos, we are automating the methodology described in this report, creating a tool that is simple to use and understand (even for those unversed in risk analysis), interactive, and portable. The fully automated interactive questionnaires in natural language make it easy to use.[3,4] The user is not required to guess at frequencies or probabilities: the expertise for this is built into a linguistic algebra based in part on fuzzy set theory.[5] Using a modular macromodel for the risk analysis on a portable personal computer instead of on a large mainframe computer and using a commercially available programming

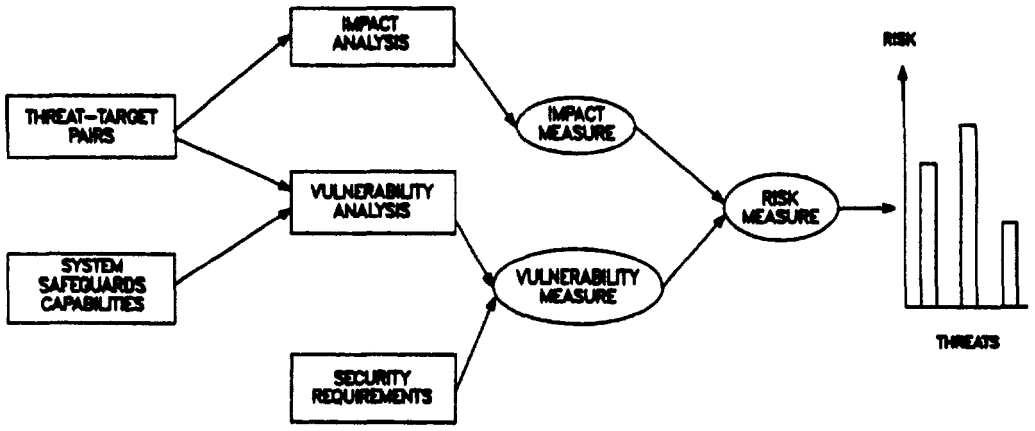


Fig. 1. Computer security risk assessment evaluates both the vulnerability to and the impact of threats succeeding against targets.

language for the software development makes our risk analysis tool totally portable and the risk analysis simple. We have applied the vulnerability assessment portion of this methodology to computer security effectiveness evaluation with good results. The method is applicable to other areas as well.

TECHNICAL APPROACH

The framework for our methodology has several steps that must be taken to create an expert system that performs risk analysis on a specific subject system. These steps are:

(1) Define the subject system (the assets, the specrum of threats, and the safeguards);
(2) Analyze the vulnerabilities;
(3) Evaluate the possible losses;
(4) Propose modifications to the safeguards system;
(5) Perform a cost-benefit analysis;
(6) Summarize in an automated report.

In our approach, the subject system definition has two major parts. First, we define a set of generic assets and a general spectrum of threats against the subject system. Then we define and model the safeguards system that protects the assets from the threats. Consider the computer security application as an example of how this is done.

To evaluate computer security safeguards effectiveness, one must identify the resources of a computer installation that could be at risk. Each of the assets is a target for one or more threats and can be damaged differently, depending on its type. In general, then, computer installation assets may be broadly classified into four categories:

(1) Installation - the building or structure housing the computer center and grounds, and the organizational structure that may be logically associated with computer center operation;
(2) Hardware - computer-related equipment such as the central processor, disk drives, tape transports, terminals, printers, video display units, shredders, office equipment, power supplies, non-computer-related equipment, and the equipment to heat, cool, and ventilate the building and the computer room;
(3) Software - any information that is stored in a form that is not easily readable by a human, such as operating systems, compilers, applications programs, data files, output files; also, the media upon which this information is stored, such as disks, tapes, memory chips;
(4) Documents/Displays - any information in a form that can be read directly by a human, including such things as hardcopy output, source listings, documentation, cards, manuals, reports, screen displays, graphics.

The vulnerability and associated risk for the subject system then can be assessed in light of a spectrum of threats whose malevolent actions upon the assets should be prevented, or at least mitigated, by the security system. Specific threats exist in many forms, such as the manipulation or disclosure of information for personal or corporate gain; deliberate destruction of property by rioters, terrorists, or disgruntled employees; errors or omissions in data files; software or hardware failures; or natural disasters like fire or flood. A threat coupled with an existing safeguards system vulnerability(ies) results in a risk increment for the subject system.

In contrast, there is no effect (or impact) on the subject system unless a threat-vulnerability pair can interact together. For example, if the subject system has no vulnerability to flood, then even a very high likelihood of flood occurrence is not significant. Similarly, if a fire is impossible in a given situation, then vulnerability to fire is not relevant.

We then can define our spectrum of threats. This spectrum can be encompassed by three generic categories:

(1) NATURAL or RANDOM HAZARDS - natural disasters such as fire, flood, seismic events, and so forth; random equipment failures; unintentional human error.
(2) DIRECT HUMAN ACTIONS - deliberate human actions to steal, modify, or destroy a given asset. These actions require that the person actually be on the premises of the subject system.
(3) INDIRECT HUMAN ACTIONS - deliberate human actions to steal, modify, or destroy a given asset. These actions are accomplished remotely and do not require that the person be on the premises of the subject system to perpetrate them.

There are two parts to defining and modeling the safeguards system. We first determine what safeguards should be in place if the system were complete. We establish what the desirable safeguards system characteristics should be and include implicit a priori decisions about the quality of the safeguards.[7,8]

To model the safeguards system, we create a comprehensive fully automated interactive questionnaire--a natural-language system that makes it easy to use.[4] The questionnaire is structured in terms of safeguards functions, safeguards elements, element attributes, and safeguards information that can be used later in the risk assessment. A safeguards functions is the function that a particular safeguard is expected to perform; an example of a safeguards function is controlling entrances and exits of the subject system's perimeter. Safeguards elements join together to accomplish the safeguards functions; an element might be the presence of a perimeter fence and another element might be the presence of monitors and alarms. Element attributes are desirable traits of the elements, and their presence (or absence) indicates the quality of that particular element; for example, attributes of the fence might include some minimum height, additional deterrents on it (like barbed wire or razor tape), and some minimum structural requirements; attributes of the monitors and alarms might be that they are on all gates, that they transmit to a staffed observation post, and that they are recorded for an audit trail to aid in reconstructing what happened if the safeguards function was breached.

A hierarchical disaggregation structure links the questionnaire with event trees for the vulnerability assessment.[6] This hierarchical decomposition relates the safeguards objectives to the threat pairs at the functional level. With each generic threat is associated a hierarchy: the top level represents the generic threat, the second level contains the generic targets, and the third level shows for each threat-target pair the safeguards functions that make up the event trees constituting the vulnerability assessment model. Figures 2-3 illustrate the concept of the hierarchical decomposition for the natural hazards threat and the direct human threat in the computer security application.

The functional event trees can be thought of as fuzzy binary event trees describing the presence and quality of the safeguards elements acting to accomplish the safeguards function represented by each tree. Figure 4 shows an event tree related to the natural hazards threat hierarchy, and Fig. 5 shows an event tree related to the direct-human threat hierarchy for the computer security application. The event trees can be traversed from one subfunction to another by two paths: either there is no control (or total non-performance of the subfunction) or there is some portion of control. The measure of the completeness of the subfunction is actually the degree of membership in the fuzzy set "subfunction operability, or presence of controls," and is normalized to be a value lying between zero and unity. This value measures the vulnerability of the safeguards performing the subfunction to the interaction of the threat-target pair.

The vulnerability measure is assigned by means of an algorithm based upon answers to questions about the safeguards elements and their attributes. A measure is determined for each safeguards attribute and then is used to determine the total vulnerability

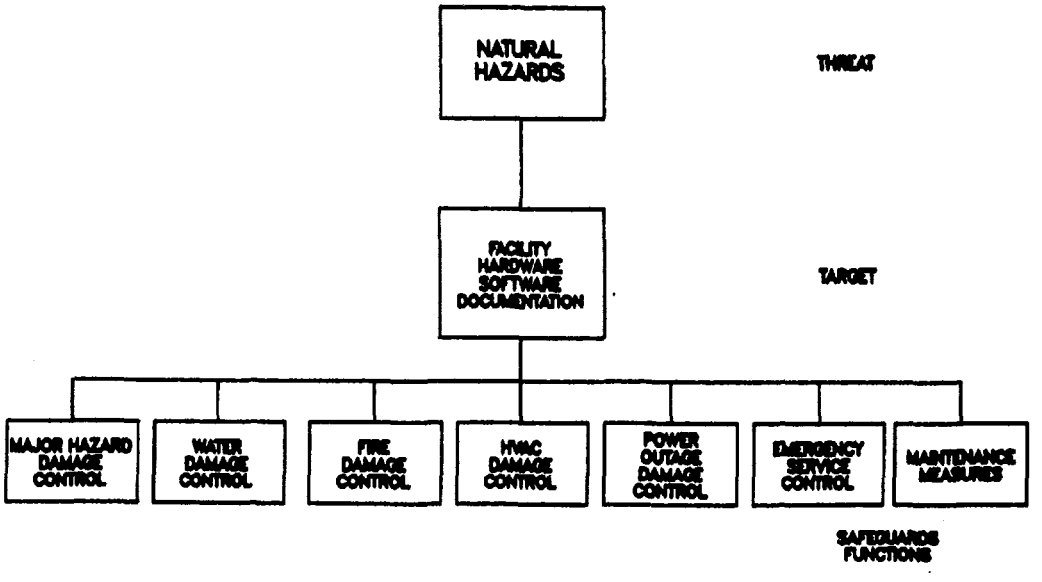


Fig. 2. Risk assessment structure for natural hazards.

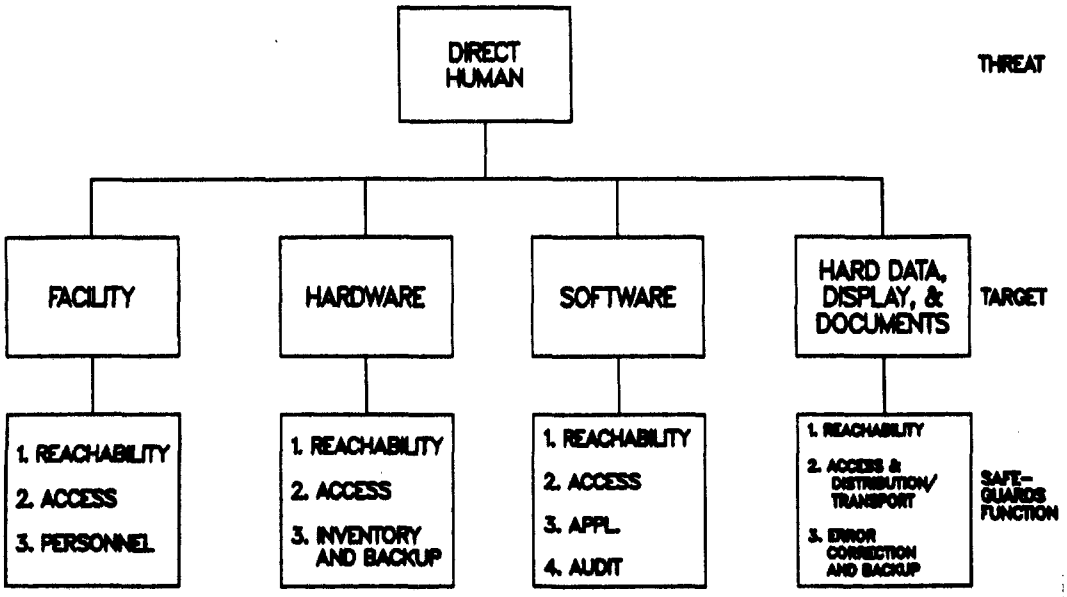


Fig. 3. Risk assessment structure for direct human adversary.

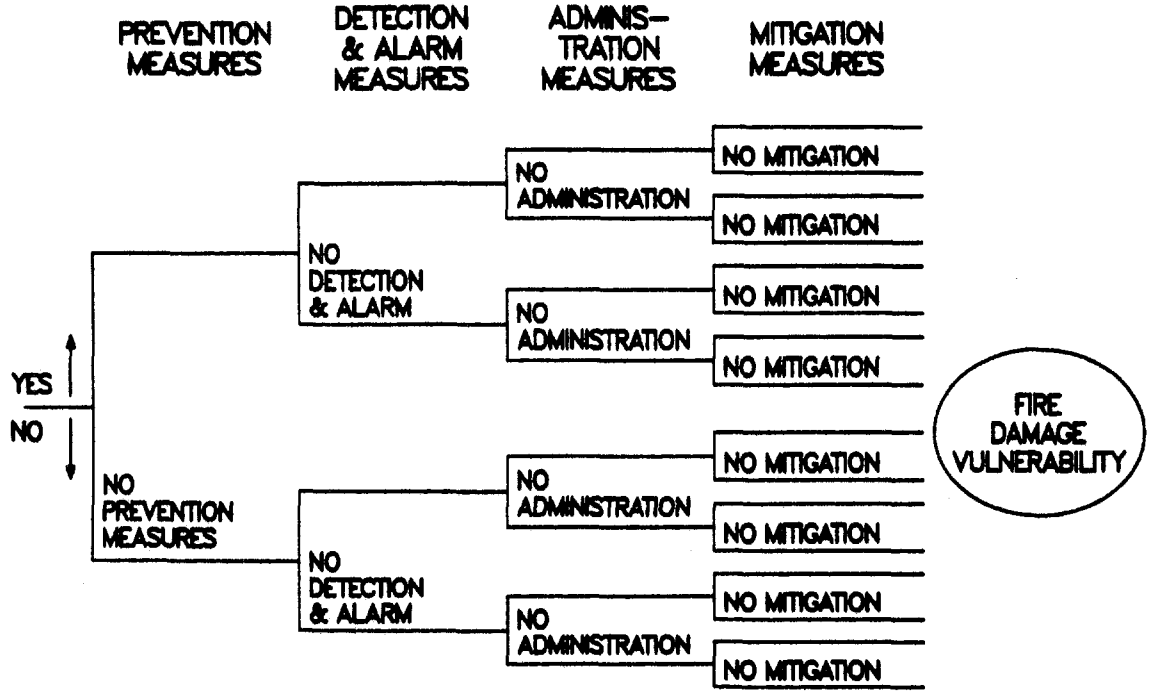


Fig. 4. Event tree for fire damage control.

measure for the associated safeguards element. The algorithm is based on the underlying assumptions that each safeguards element required to perform a specific safeguards subfunction is approximately equal in importance to one another, and that each attribute required for completeness of a specific element is equal in importance to the other attributes of that element. The normalized value arises from aggregating the attribute measures to arrive at a measure for each element, aggregating the measures for the elements contributing to the performance of a particular subfunction and then normalizing the total aggregated measure relative to the number of elements contributing to that subfunction. An organization-specific linguistic vulnerability measure (such as "very high" or "low") can be scaled from the quantitative measure by

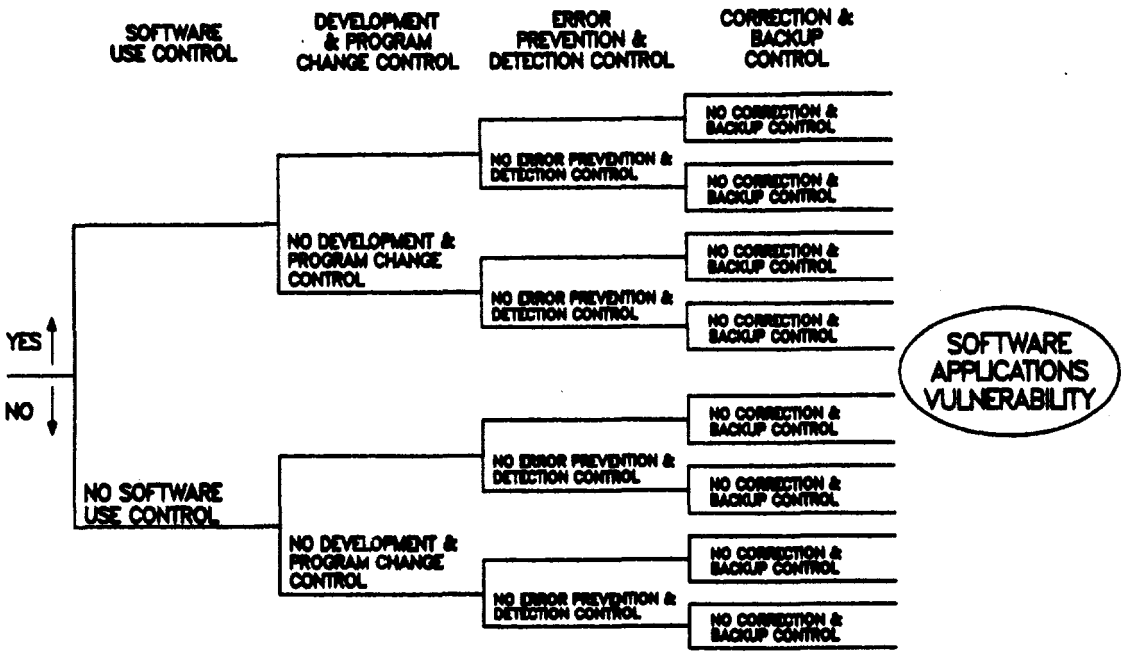


Fig. 5. Event tree for software applications control.

eliciting information about the sensitivity of the work that the organization does.

To assess the potential effect of a breached safeguards function on the organization, we first define a spectrum of generic outcome scenarios for the pairwise combinations of the generic threats and generic targets.

Then, for each outcome for each threat-target pair, we evaluate how such an outcome might affect the organization (the impact severity),[9,10] taking into account such application-specific considerations as the relative importance of the target and contingency plans. An event-tree structure is used to determine the organization-specific impacts based upon the possible outcomes, and both monetary and non-monetary costs are used to measure the severity of the impacts.

To illustrate this concept with examples from the computer security application, let us assume the Direct Human threat is the malefactor. If the target is the installation, the safeguards functions include perimeter control, building control, area control, general access control, awareness, employee-status monitoring, security and emergency training, and emergency service monitoring. An example of an outcome set for perimeter control is unauthorized access, tampering or damage, and destruction.

A non-monetary measure for impact severity is obtained by eliciting information about how a specific member of the outcome set affects the organization with respect to such considerations as adverse public reaction, embarrassment to the organization, organizational disruption or loss of morale, unsafe operating conditions, and national security implications. A monetary measure is obtained in the same way, except that in this instance the considerations include loss of contracts, fraud or embezzlement, operations interruption, and termination of operations. We can derive a linguistic measure for impact severity after considering the monetary costs (of investigation and followup, disruption of activities, replacement, and personnel injury) and the non-monetary costs (of injured personnel, hoax, and public knowledge).

A probabilistic linguistic algebra matrix then maps vulnerability and impact into risk. The linguistic values used are VL (very low), L (low), M (medium), H (high), and VH (very high). This mapping, skewed toward impact (or weighting impact more than vulnerability), indicates normal human and organizational aversion to risk. In other words, the magnitude of the vulnerability is not as important to most persons or organizations as how the exploited vulnerability might affect (or cost) them.

CONCLUSIONS

Our original methodology is technically sound, accurate, simple to understand, interactive, and portable. The accuracy is derived from exhaustive and comprehensive questions that the developer of specific applications provides. The interactive conversational questionnaire in natural language is straightforward. The functional structure of the model makes decision-making simple, clearly indicates what safeguards are missing, and provides a rationale for selecting the safeguards to add. The implementation is compatible with standard IBM-PC software, making the system portable.

The vulnerability assessment portion of this methodology has been automated (including an automated report generator) and is currently being used by the Nuclear Regulatory Commission and the National Bureau of Standards, and is being tested at selected sites in the Department of Energy complex and the Federal Bureau of Investigation. Further development and automation of our methodology is continuing as funding permits.

After suitable development to make our framework consistent with a specific application, our methodology can be used to determine vulnerabilities and risks inherent in such applications systems as computer systems,[11,12] material control applications systems,[13] physical protection systems, plant process-control systems,[14] security systems, and a host of others.

REFERENCES

1. Rowe, W. D. (1977). An Anatomy of Risk. John Wiley and Sons, Inc., New York.
2. McCormick, N. J. (1981). Reliability and Risk Analysis: Methods and Nuclear Power Applications. Academic Press, New York.
3. Negoita, C. V. (1985). Expert Systems and Fuzzy Systems. The Benjamin/Cummings Publishing Company, Inc., Menlo Park, California.
4. Sudman and Bradburn, N. M. (1982). Asking Questions: A Practical Guide to Questionnaire Design. Jossey-Bass, Inc., San Francisco.
5. Zadeh, L. A., Fu, K.-S., Tanaka, K. and Shimura, M. (1975). Fuzzy Sets and Their Applications to Cognitive and Decision Processes. Academic Press, New York.
6. Mesarovic, M. D., Macks, D., and Takahara, Y. (1970). Theory of Hierarchical Multilevel Systems. Academic Press, New York and London.
7. Jain, R. (January, 1977). A Procedure for Multiple-Aspect Decision-Making Using Fuzzy Sets. INT. J. SYSTEMS SCI. 8(1): 1-7.
8. Bellman, R. E. and Zadeh, L. A. (December, 1970). Decision-Making in a Fuzzy Environment. MANAGEMENT SCIENCE. 17(4).
9. Johnson, E. M. and Huber, G. P. (May 1977). The Technology of Utility Assessment. IEEE TRANS. SYS., MAN., CYBER. SMC-7(5).
10. Schoemaker, P. J. H. and Waid, D. C. (February, 1982). An Experimental Comparison of Different Approaches to Determining Weights in Additive Utility Models. MANAGEMENT SCIENCE. 28(2).
11. Smith, S. T. and Lim, J. J. (1984). Computer Security Evaluation Tools. Seventh DOE Computer Security Group Conference, New Orleans, April 17-19, 1984.
12. Smith, S. T. and Lim, J. J. (1984). An Automated Method for Assessing the Effectiveness of Computer Security Safeguards. IFIP Second International Congress on Computer Security, Toronto, Canada, September 10-12, 1984.
13. Smith, S. T. and Lim, J. J. (1984). "An Automated Procedure for Performing Computer Security Risk Analysis," Proceedings Sixth Annual Symposium on Safeguards and Nuclear Material Management. ESARDA 17: 527-530.
14. Smith, S. T. and Lim J. J. (1984). Assessment of Computer Security Effectiveness for Safe Plant Operation," ANS 1984 Annual Meeting, New Orleans, Louisiana, June 3-8, 1984.

LA-UR-86-2282

Los Alamos National Laboratory is operated by the University of California for the United States Department of Energy under contract W-7405-ENG-36.

TITLE: LAVA - A CONCEPTUAL FRAMEWORK FOR AUTOMATED RISK ASSESSMENT

AUTHOR(S): S. T. Smith, D. C. Brown, T. H. Erkkila, P. D. FitzGerald, J. J. Lim, L. Massagli, J. R. Phillips, and R. M. Tisinger

SUBMITTED TO: Proceedings of the 27th Annual Meeting of the Institute of Nuclear Materials Management

By acceptance of this article, the publisher recognizes that the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes.

The Los Alamos National Laboratory requests that the publisher identify this article as work performed under the auspices of the U.S. Department of Energy.

Los Alamos Los Alamos National Laboratory
Los Alamos, New Mexico 87545

FORM NO. 836 R4
ST NO. 2629 5/81

LAVA - A CONCEPTUAL FRAMEWORK FOR AUTOMATED RISK ASSESSMENT*

S. T. Smith, D. C. Brown,** T. H. Erkkila, P. D. FitzGerald,**
J. J. Lim, L. Massagli, J. R. Phillips, and R. M. Tisinger

Los Alamos National Laboratory

Los Alamos, NM 87545

ABSTRACT

At the Los Alamos National Laboratory we are developing the framework for generating knowledge-based systems that perform automated risk analyses on an organization's assets. An organization's assets can be subdivided into tangible and intangible assets. Tangible assets include facilities, materiel, personnel, and time, while intangible assets include such factors as reputation, employee morale, and technical knowledge. The potential loss exposure of an asset is dependent upon the threats (both static and dynamic), the vulnerabilities in the mechanisms protecting the assets from the threats, and the consequences of the threats successfully exploiting the protective systems vulnerabilities. The methodology is based upon decision analysis, fuzzy set theory, natural-language processing, and event-tree structures. The Los Alamos Vulnerability and Risk Assessment (LAVA) methodology has been applied to computer security. LAVA is modeled using an interactive questionnaire in natural language and is fully automated on a personal computer. The program generates both summary reports for use by both management personnel and detailed reports for use by operations staff. LAVA has been in use by the Nuclear Regulatory Commission and the National Bureau of Standards for nearly two years and is presently under evaluation by other governmental agencies.

INTRODUCTION

The goals and objectives of a risk management program are defined by both external and internal requirements. External requirements arise from guidelines or rules issued by governmental agencies and legal responsibilities of the organization, as well as constraints placed upon the organization by society. Internal requirements arise from consideration of such factors as organizational vitality, profitability, and moral responsibility. Both sets of requirements must be considered during the formulation of an organization's risk management program.

*This work was supported by the Department of Energy, Office of Safeguards and Security.

**Employed by the U.S. Government.

There are three basic components to an effective risk management program: (1) identification of the assets, (2) identification of the potential threats, and (3) reduction of potential loss exposure by defining the set of safeguards functions (mechanisms, policies, and procedures) that safeguard the asset from the threat. By using this approach, we eliminate the necessity for defining elaborate scenarios (where we are not assured that the scenario set is complete), eliminate the requirement of estimating event probabilities from a set of inadequate or incomplete data, and measure the consequences more accurately by using both monetary and nonmonetary (or linguistic) descriptors.[1-5]

Identification of Assets

The assets must be defined precisely before any risk management program can be established. Oftentimes an organization's assets are vaguely defined as "those things that make up" the organization. This type of definition is not satisfactory for risk management. Generally, the assets can be subdivided into two categories: tangible assets and intangible assets. Tangible assets include facilities, materiel, personnel, and time. Intangible assets are more difficult to define precisely but can be as or more important than the tangible assets. Intangible assets include organizational reputation, employee motivation and morale, and the technological basis of an organization. An asset may be, at the same time, both tangible and intangible. An employee is a tangible asset, while his technical knowledge and motivation are intangible assets.

Identification of Potential Threats

To define the potential for loss exposure to an organization and its assets, a threat analysis must first determine the existence of potential threats taking into account possible threat agents and their potential targets. The threat component consists of two parts: the static (or relatively constant background) threat, and the dynamic (or changing) threat. The threat component measures the relative strengths of identifiable threat agents in terms of motivation, opportunity, and capability against the safeguards functions (the functional objectives of the controls and mechanisms that protect the assets from the threats).

LOS ALAMOS VULNERABILITY AND RISK ASSESSMENT METHODOLOGY - LAVA

The Los Alamos Vulnerability and Risk Assessment Methodology (LAVA) is a systematic method for assessing vulnerabilities in safeguards systems. We have applied the LAVA methodology to model supply and property systems, control systems for awarding and administrating contracts, international communications and information flow systems,[7] and computer security systems. We have implemented the vulnerability assessment portion for computer security and are presently implementing the consequence analysis portion. The LAVA implementation yields qualitative insights into the vulnerabilities of computer systems to natural hazards and on-site human threat agents. The assessment process is based upon a team approach for the evaluation of the vulnerabilities of established safeguards functions at a facility.

A. Definition of Threat/Asset Pairs

For computer security we have defined four general categories of tangible assets: facility, hardware, software, and documentation. The facility includes the physical structure of the computer facility, adjacent supporting facilities (air-conditioning units, power distribution stations), and personnel. Hardware is restricted to the physical parts of the computer system, like central processing unit, disk drives, printers, and terminals. Software (or machine-readable information) includes both commercially produced software as well as internally produced software and information. Documents (or human-readable information) consist of manuals, printer/plot output information, and display screens.

We have identified three threat agents for these four categories of assets: natural hazards, on-site human (the agent must be physically present), and off-site human (the agent is not physically present; for example, the agent can access the computer system through dial-up lines). For the unclassified version of LAVA we address only the static component of the natural hazards and the on-site human threat agents. The interaction of these threat agents with the previously defined assets is represented in Fig. 1. The natural hazard threat agent does not distinguish between the assets--it "attacks" all the assets without discrimination. Therefore, the threat/asset pair for natural hazards is the same for all combinations. However, given the case of the on-site human threat agent, there are unique threat/asset pairs that must be considered when the vulnerabilities of the computer facility are evaluated. There is a unique set of safeguards functions that should be in place to protect each of the categories of assets. A few safeguards functions are common to all four categories of assets.

B. Definition of the Safeguards Functions

A unique set of safeguards functions is associated with each threat/asset pair. As discussed in the previous sections, each safeguards function may be composed of several subfunctions. There

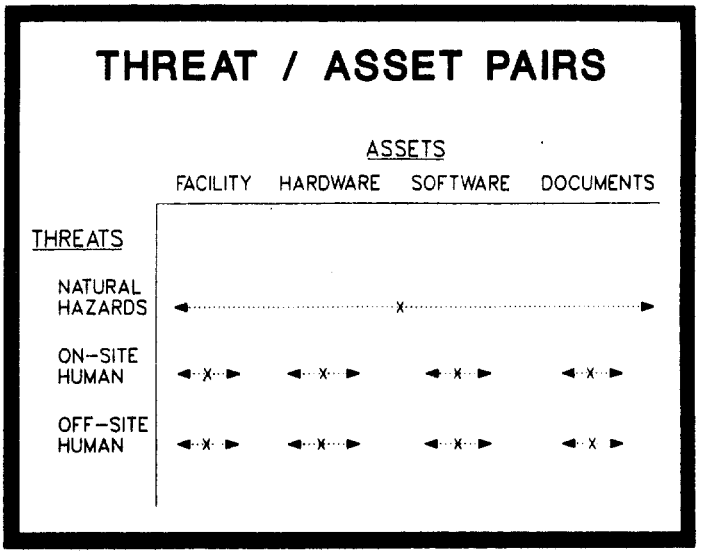


Fig. 1.
Threats from natural hazards are indiscriminate, affecting all assets equally. On-site and off-site human threats can target specific assets or groups of assets.

is an optimal set of safeguards functions to protect a specific asset from a specific threat. The adequacy and completeness of these functions and subfunctions are determined by evaluating the presence or absence of elements and attributes by answering a set of specially designed questions. The responses to these questions measure the degree to which the elements and attributes are complete.

C. Evaluation of the Vulnerabilities of Safeguards Functions

The evaluation process is based upon a team approach. This approach is vital for arriving at results that are real and interpretable. The quality of the assessment depends upon the quality of the team members. The broader the spectrum of the backgrounds and expertise of the team members, the better (and more accurate) the assessment will be. There are two parts to the team: a core team whose members are present throughout the entire assessment period, and a transient team whose members attend only during those times their expertise is required. The team members should have specialized knowledge about different aspects of the facility and its assets. Desirable backgrounds or expertise for the team members include physical security, technical security, building engineering, software development, communication systems, computer operations, and other areas of expertise.

There are four parts to the assessment process. The first part consists of a review of the computer installation to be assessed. A visit to the facility is completed by the entire assessment team. The components (or assets) are identified, procedures and policies are discussed, and individuals that the assessment team can contact for

Appendix D

Questionnaire

- LAVA/COMPUTER SECURITY VULNERABILITY ASSESSMENT QUESTIONNAIRE -

S. T. Smith (Principal Investigator), et al

Copyright (C) 1983,1986 The Regents of the University of California

NATURAL HAZARDS MODULES:

Major Hazards	- Exposure, Resistance
Water Damage	- Prevention, Detection, Mitigation
Fire Damage	- Prevention, Detection, Administration, Mitigation
HVAC Damage	- Prevention, Detection, Mitigation
Power Outage Damage	- Prevention, Detection, Mitigation
Emergency Service	- Emergency Alert, Emergency Response
Maintenance	- Preventive Maintenance, Housekeeping

DIRECT HUMAN MODULES:

Reachability (all 4)	- Perimeter, Building, Area, Room
Facility/Org. Access	- Gen. Access, Visitor/Vendor/Service, Authorization
Facility Personnel	- Management Awareness, Employee Status Monitoring, Security & Emergency Training, Emergency Service Personnel Monitoring
Hardware Access	- Physical, Vendor/Service Maintenance, Authorizat'n
Hdware Inventory/Backup	- Inventory & Audit, Backup
Software Access	- Physical, Login Proc., Operating System Proc.
Software Applications	- Software Use, Development & Program Change, Error Prevention & Detection, Correction & Backup
Software Audit	- Internal Audit, Data Traceability
HDDD Access/Dist/Trans	- Access Control, Distribution & Transport
HDDD ErrCorr & Backup	- Error Correction, Backup

CATEGORY #	CATEGORY NAME	NUMBER OF QUESTIONS
1	Area Entry & Authorization	30
2	Area Procedure & Policy	30
3	Building Construction	33
4	Building Engineering	33
5	Building Entry & Authorization	55
6	Communications	12
7	Computer Operating System	25
8	Computer Operations	20
9	Computer Room Construction	32
10	Computer Room Contents	33
11	Computer Room Entry	54
12	Computer Room Procedures & Policy	43
13	Computer Room Raised Floor	28
14	Computer Room Sensors & Alarms	25
15	Computer Room Suspended Ceiling	14
16	Data Center Management	62
17	Data Traceability	13
18	Emergency & Contingency Planning	44
19	Emergency Situations & Procedures	61
20	Encryption	3
21	Files, Storage Media, & Drives	21
22	General Locale	20
23	Heating, Ventilation, & Air Conditioning	29
24	Housekeeping & Maintenance	16
25	Inventory Procedures & Policy	11
26	Management Issues & Policy	60
27	Negotiable Financial Documents	8
28	Passwords	47
29	Perimeter Zone	62
30	Personnel Privacy	10
31	Storage Media Library	16
32	Terminals	13
33	Transportation	6
34	Visitors, Vendors, & Service Personnel	29

```
**********************************************************************
**          - LAVA/CS VULNERABILITY ASSESSMENT QUESTIONNAIRE -       **
**                                                                   **
**                                                                   **
**           S. T. Smith (LAVA Principal Investigator), et al.       **
**                                                                   **
**                                                                   **
**       Copyright (C) 1983, 1987  Los Alamos National Laboratory    **
**********************************************************************
```

The questions are numbered as XX.YY, where XX is the category number and YY is the question identifier within the category.

Category 1 : AREA ENTRY & AUTHORIZATION

1. 1 Does a barrier(s) (such as walls, partitions, or partial walls, even if the AREA is an integral part of the computer ROOM) separate the computer AREA from the rest of the BUILDING?
YES -> jump 1 , NO -> jump 30

1. 2 Is the construction of the AREA barrier adequately strong to perform the function for which it is intended?
YES -> jump 1 , NO -> jump 1

1. 3 Is the AREA barrier fire-resistant?
YES -> jump 1 , NO -> jump 1

1. 4 Is entry to the computer AREA controlled separately from the BUILDING or computer ROOM controls? (An affirmative answer will lead to a series of questions about HOW and WHEN it is controlled.)
YES -> jump 1 , NO -> jump 27

1. 5 Is computer AREA entry controlled at ANY time?
YES -> jump 1 , NO -> jump 5

1. 6 Is computer AREA entry controlled when the computer itself is unattended?
YES -> jump 1 , NO -> jump 1

1. 7 Is computer AREA entry controlled DURING normal working hours?
YES -> jump 1 , NO -> jump 1

1. 8 Is computer AREA entry controlled OUTSIDE OF normal working hours?
YES -> jump 1 , NO -> jump 1

1. 9 Is computer AREA entry controlled DURING EMERGENCY situations?
YES -> jump 1 , NO -> jump 1

1.10 Are emergency exits from the computer AREA operable only from within?
YES -> jump 1 , NO -> jump 1

1.11 Is computer AREA entry controlled by a GUARD(s) or other individuals?
YES -> jump 1 , NO -> jump 2

1.12 Does the guard or other individual control computer AREA entry by a) visual recognition, b) verifying ID from a list, c) badge with no photo, d) badge with photo, e) other (specify).
YES -> jump 1 , NO -> jump 1

1.13 Is computer AREA entry controlled by a KEY?
YES -> jump 1 , NO -> jump 3

1.14 How many persons have keys to the computer AREA?
YES -> jump 1 , NO -> jump 1

1.15 Is it difficult to duplicate computer AREA keys (ie, do keys have engraved instructions to prohibit their duplication, are they made on special blanks not available to others, etc.)?
YES -> jump 1 , NO -> jump 1

1.16 Is computer AREA entry controlled by CIPHER LOCK(s)?
YES -> jump 1 , NO -> jump 3

1.17 How many persons know the combination to the computer AREA cipher locks?
YES -> jump 1 , NO -> jump 1

1.18 Are combinations for the computer AREA cipher locks changed on a regular basis?
YES -> jump 1 , NO -> jump 1

1.19 Is computer AREA entry controlled by MAGNETIC BADGE/CARD/KEY-CARD READERS?
YES -> jump 1 , NO -> jump 2

1.20 How many persons have magnetic cards, badges, or key cards permitting entry to the computer AREA?
YES -> jump 1 , NO -> jump 1

1.21 Are security personnel notified of employes who are permitted to enter the computer AREA outside of normal working hours?
YES -> jump 1 , NO -> jump 1

1.22 Are there effective procedures for authorizing AREA entry?
YES -> jump 1 , NO -> jump 3

1.23 Is there a designated individual responsible for authorizing AREA entry?
YES -> jump 1 , NO -> jump 2

1.24 State who is responsible for authorizing AREA entry.
YES -> jump 1 , NO -> jump 1

1.25 Is there a procedure to control badges, keys, combinations, and/or cards used for entry to the computer AREA?
YES -> jump 1 , NO -> jump 1

1.26 Are authorization lists and control mechanisms permitting computer AREA entry updated when a person's AREA entry authority is revoked?
YES -> jump 1 , NO -> jump 2

1.27 When a person's AREA entry authorization is revoked, are a) authorization lists revised, b) locks/combinations changed, c) badges, keys, cards surrendered, d) other (specify).
YES -> jump 1 , NO -> jump 1

1.28 Is access to AREA resources denied quickly enough to prevent damage to the resources by a person whose AREA entry authorization has been revoked?
YES -> jump 1 , NO -> jump 1

1.29 Do employes challenge persons in the computer AREA if these persons are not properly identifiable?
YES -> jump 1 , NO -> jump 1

1.30 Are there procedures permitting computer AREA access to emergency personnel in case of fire, major power outage, or other emergency or disaster?
YES -> jump 1 , NO -> jump 1

Category 2 : AREA PROCEDURE & POLICY

2. 1 Is there a record of entries to and exits from the computer AREA by employes (excluding the assigned operations staff)?
YES -> jump 1 , NO -> jump 5

2. 2 Is there a record of entries to and exits from the computer AREA by employes (excluding the assigned operations staff) DURING normal working hours?
YES -> jump 1 , NO -> jump 1

2. 3 Is there a record of entries to and exits from the computer AREA by employes (excluding the assigned operations staff) during emergencies and non-normal working hours?
YES -> jump 1 , NO -> jump 1

2. 4 The means used to record employe entries to & exits from the computer AREA are: a) magnetic key card, b) sign-in register, c) other.
YES -> jump 1 , NO -> jump 1

2. 5 Does the AREA employe entry/exit record provide notation for time in, time out, identification of entrant, and authorization mechanism?
YES -> jump 1 , NO -> jump 1

2. 6 Are entries/exits by non-employes to the computer AREA recorded?
YES -> jump 1 , NO -> jump 5

2. 7 Are entries/exits by non-employes to the computer AREA recorded DURING normal working hours?
YES -> jump 1 , NO -> jump 1

2. 8 Are entries/exits by non-employes to the computer AREA recorded during emergencies and non-normal working hours?
YES -> jump 1 , NO -> jump 1

2. 9 The means used to record non-employe entries/exits to the computer AREA are: a) magnetic key card, b) sign-in register, c) other.
YES -> jump 1 , NO -> jump 1

2.10 Does the AREA non-employe entry/exit record provide notation for time in, time out, identification of entrant, and authorization mechanism?
YES -> jump 1 , NO -> jump 1

2.11 Are there monitors (e.g., CCTV, guards, etc.) and alarms for the computer AREA entrances?
YES -> jump 1 , NO -> jump 10

2.12 Do monitors operate for normal operating entrances to the computer AREA?
YES -> jump 1 , NO -> jump 1

2.13 Do monitors operate for emergency exits and emergency situations in the computer AREA?
YES -> jump 1 , NO -> jump 1

2.14 Do monitors operate for other non-normal entrances/exits (such as delivery portals) to the computer AREA?
YES -> jump 1 , NO -> jump 1

2.15 Do computer AREA monitors and alarms transmit to a location where timely appropriate action will be taken?
YES -> jump 1 , NO -> jump 2

2.16 Where do computer AREA monitors and alarms transmit? a) a main guard station off-site, b) a guard station in another building, c) a guard station in the same building, d) other.
YES -> jump 1 , NO -> jump 1

2.17 Are there documented guidelines for evaluating appropriate responses to notifications from AREA entrance monitors and/or alarms?
YES -> jump 1 , NO -> jump 1

2.18 Are appropriate procedures for responding to a notification from AREA monitors and alarms defined and documented?
YES -> jump 1 , NO -> jump 1

2.19 Are personnel trained or drilled in how to respond to AREA monitors and alarms?
YES -> jump 1 , NO -> jump 1

2.20 Is a record from computer AREA monitors and alarms kept in some form available for audit?
YES -> jump 1 , NO -> jump 1

2.21 Are intrusion sensors or other intrusion detection devices used within the computer AREA?
YES -> jump 1 , NO -> jump 4

2.22 Sensor devices used in the computer AREA are: a) motion detectors, b) door switches, c) breakwire sensors, d) vibration sensors, e) closed-circuit TV, f) other.
YES -> jump 1 , NO -> jump 1

2.23 Is output from the intrusion sensors and/or detection devices transmitted outside the computer AREA?
YES -> jump 1 , NO -> jump 2

2.24 Indicate the location(s) to which the intrusion sensors and/or detection devices transmit output: a) main security station, b) building security station, c) municipal police station, d) other.
YES -> jump 1 , NO -> jump 1

2.25 Are there enforced procedures for controlling equipment, parts, storage media, storage devices, and documentation removal from the computer AREA?
YES -> jump 1 , NO -> jump 5

2.26 Are there enforced procedures for controlling equipment removal from the computer AREA?
YES -> jump 1 , NO -> jump 1

2.27 Are there enforced procedures for controlling storage-media and storage-device removal from the computer AREA?
YES -> jump 1 , NO -> jump 1

2.28 Are there enforced procedures for controlling equipment parts removal from the computer AREA?
YES -> jump 1 , NO -> jump 1

2.29 Are there enforced procedures for controlling documents removal from the computer AREA?
YES -> jump 1 , NO -> jump 1

2.30 Are personnel work areas within the computer AREA monitored for unauthorized use?
YES -> jump 1 , NO -> jump 1

Category 3 : BUILDING CONSTRUCTION

3. 1 Is the data center housed in something other than a permanent BUILDING?
YES -> jump 1 , NO -> jump 2

3. 2 In what is the data center housed? a) a semi-permanent transportable building, b) a trailer, c) a RV, d) other (specify).
YES -> jump 1 , NO -> jump 1

3. 3 Is the BUILDING constructed on a solid foundation?
YES -> jump 1 , NO -> jump 1

3. 4 Is the principal material of the EXTERIOR walls of the BUILDING housing the data center one of the following materials: reinforced concrete, concrete block, brick, or stone?
YES -> jump 2 , NO -> jump 1

3. 5 What is the material of the EXTERIOR walls of the BUILDING: a) wood, b) stucco, or c) other material.
YES -> jump 1 , NO -> jump 1

3. 6 Is the principal material of the doors and/or gates entering into the BUILDING either metal or metal clad?
YES -> jump 2 , NO -> jump 1

3. 7 What is the construction of the exterior BUILDING doors: a) solid wood, b) hollow-core wood, c) glass, or d) other material.
YES -> jump 1 , NO -> jump 1

3. 8 Is the principal material of the INTERIOR walls of the BUILDING one of the following materials : reinforced concrete, concrete block, brick, or metal?
YES -> jump 2 , NO -> jump 1

3. 9 What is the material of the INTERIOR walls of the BUILDING: a) sheetrock, b) plaster, c) veneer on plywood, d) ceramic tile, or e) other material.
YES -> jump 1 , NO -> jump 1

3.10 Is the principal material of the BUILDING's ceilings/floors reinforced concrete or metal?
YES -> jump 2 , NO -> jump 1

3.11 What best describes the BUILDING's surface ceiling material: a) gypsum, b) wood, c) wallboard, d) acoustical tile, e) exposed structure, or f) other material.
YES -> jump 1 , NO -> jump 1

3.12 Do the data center's walls and penetrations have a fire rating of at least 2 hours?
YES -> jump 2 , NO -> jump 1

3.13 What is the fire rating of the data center's walls and penetrations?
YES -> jump 1 , NO -> jump 1

3.14 Has the BUILDING housing the data center more than one story?
YES -> jump 1 , NO -> jump 5

3.15 How many floors of the BUILDING are above grade?
YES -> jump 1 , NO -> jump 1

3.16 How many floors of the BUILDING are below grade?
YES -> jump 1 , NO -> jump 1

3.17 On what floor of the BUILDING is the data center located?
YES -> jump 1 , NO -> jump 1

3.18 Is the floor upon which the data center is located either at or below grade?
YES -> jump 1 , NO -> jump 1

3.19 Does either (or both) grading around the exterior of the building or storm drains remove water accumulation during sudden or seasonal heavy rainfall?
YES -> jump 1 , NO -> jump 1

3.20 Have roof, upper floor, and foundation drainage devices been installed for the data center?
YES -> jump 1 , NO -> jump 1

3.21 Is the roof above the data center watertight?
YES -> jump 1 , NO -> jump 5

3.22 Is the BUILDING roof constructed to prevent opening (and subsequent water leakage) caused by high winds?
YES -> jump 1 , NO -> jump 1

3.23 Is there protection against accumulated air-conditioning water, leaks in rooftop cooling towers, or other water sources?
YES -> jump 1 , NO -> jump 1

3.24 Are all roof penetrations (such as those for pipes, vents, antennae, etc.) sealed to prevent water leakage?
YES -> jump 1 , NO -> jump 1

3.25 Are the computer and associated hardware located so that they will not be damaged by any water leakage from the roof?
YES -> jump 1 , NO -> jump 1

3.26 Are there drains installed on the surface (roof or floor) above the computer center to divert accumulated water away from all hardware?
YES -> jump 1 , NO -> jump 1

3.27 Are there additional floors/attics/storage areas in use above the data center?
YES -> jump 1 , NO -> jump 6

3.28 Is the structural ceiling above the data center watertight?
YES -> jump 1 , NO -> jump 4

3.29 Is there protection against accumulated water leaking into the data center from the floor above?
YES -> jump 1 , NO -> jump 1

3.30 Are openings or penetrations through the roof or floor above the data center sealed against water penetration?
YES -> jump 1 , NO -> jump 1

3.31 Are the computer and associated hardware located away from known water sources on floors above?
YES -> jump 1 , NO -> jump 1

3.32 Are there drains installed on the floor above the data center to divert accumulated water away from all hardware?
YES -> jump 1 , NO -> jump 1

3.33 Are the building's transformers, motor generators, breaker panels, cooling towers, etc., protected from unauthorized access?
YES -> jump 1 , NO -> jump 1

Category 4 : BUILDING ENGINEERING

4. 1 Should the data center have an isolated and regulated power service?
YES -> jump 1 , NO -> jump 2

4. 2 Does the data center have an isolated and regulated power service?
YES -> jump 1 , NO -> jump 1

4. 3 Does the kind of data processing done at the data center require an uninterruptible power supply?
YES -> jump 1 , NO -> jump 2

4. 4 Does the data center have an uninterruptible power supply?
YES -> jump 1 , NO -> jump 1

4. 5 Does the data center have any protection against power abnormalities (e.g., line filters, either isolation or constant-voltage transformers, motor generators)?
YES -> jump 1 , NO -> jump 5

4. 6 Does the data center have power-line filters?
YES -> jump 1 , NO -> jump 1

4. 7 Does the data center have isolation transformers?
YES -> jump 1 , NO -> jump 1

4. 8 Does the data center have constant-voltage transformers?
YES -> jump 1 , NO -> jump 1

4. 9 Does the data center have motor-driven generators?
YES -> jump 1 , NO -> jump 1

4.10 Are emergency power-offs at the data center protected from accidenta activation?
YES -> jump 1 , NO -> jump 1

4.11 Has the local power supply been determined to be adequate, consistent, and reliable?
YES -> jump 1 , NO -> jump 1

4.12 Does the data center have standby power for electrically-controlled doors, security systems, OR alarms in case of power outages (Y will elicit information about each)?
YES -> jump 1 , NO -> jump 5

4.13 Does the data center have standby power for electrically-controlled DOORS in case of power outages?
YES -> jump 1 , NO -> jump 1

4.14 Does the data center have standby power for electrically-controlled SECURITY SYSTEMS in case of power outages?
YES -> jump 1 , NO -> jump 1

4.15 Does the data center have standby power for electrically-controlled ALARMS in case of power outages?
YES -> jump 1 , NO -> jump 1

4.16 Is the standby power for electrically-controlled doors, security systems, and alarms tested at regular intervals determined by site management?
YES -> jump 1 , NO -> jump 1

4.17 Is manual intervention required to restore power to the data center following a power interruption?
YES -> jump 1 , NO -> jump 1

4.18 Is there emergency lighting available for the data center if a power failure should occur?
YES -> jump 1 , NO -> jump 3

4.19 Does the data center have a separate emergency lighting system that activates when the main lighting fails?
YES -> jump 1 , NO -> jump 1

4.20 Is the data center's emergency lighting system tested on a regularly-scheduled basis?
YES -> jump 1 , NO -> jump 1

4.21 Is the data center's power supply monitored to detect the occurrence of electrical transients?
YES -> jump 1 , NO -> jump 2

4.22 Is there an immediate or automatic response when electrical transients are detected by the data center's power-supply monitor?
YES -> jump 1 , NO -> jump 1

4.23 Are all electrical cables and wiring in the BUILDING located away from normal traffic paths or protected from being disturbed by traffic?
YES -> jump 1 , NO -> jump 1

4.24 Are BUILDING transformers, motor generators, breaker panels, cipher-lock door overrides, etc., protected from unauthorized access?
YES -> jump 1 , NO -> jump 1

4.25 Is a water-detection system installed and used in the BUILDING?
YES -> jump 1 , NO -> jump 1

4.26 Does the BUILDING have a functioning flood control pump or sump pump?
YES -> jump 1 , NO -> jump 1

4.27 Is the BUILDING housing the data center equipped with operational lightning arrestors?
YES -> jump 1 , NO -> jump 1

4.28 Does the BUILDING in which the data center is housed have ductwork?
YES -> jump 1 , NO -> jump 6

4.29 Are air-conditioning duct linings and filters non-combustible?
YES -> jump 1 , NO -> jump 1

4.30 Are there automatic fire dampers in the BUILDING ductwork?
YES -> jump 1 , NO -> jump 1

4.31 Is the ducting large enough and sturdy enough to permit the passage of a person through it?
YES -> jump 1 , NO -> jump 2

4.32 Are openings to all ducting blocked securely to restrict entry to th computer ROOM by means of the ducting?
YES -> jump 1 , NO -> jump 1

4.33 Are smoke/fire DETECTORS installed in the air-conditioning return ducts?
YES -> jump 1 , NO -> jump 1

Category 5 : BUILDING ENTRY & AUTHORIZATION

5. 1 Is there a designated individual responsible for authorizing BUILDIN entry?
YES -> jump 1 , NO -> jump 2

5. 2 State who is responsible for authorizing BUILDING entry.
YES -> jump 1 , NO -> jump 1

5. 3 Are there effective procedures for authorizing BUILDING entry?
YES -> jump 1 , NO -> jump 1

5. 4 Are there effective procedures for authorizing BUILDING entry for abnormal situations (emergencies, outside of normal hours, etc.)?
YES -> jump 1 , NO -> jump 1

5. 5 Is there an independent verification of a request for BUILDING entry authorization?
YES -> jump 1 , NO -> jump 1

5. 6 Is positive identification required for a person to receive BUILDING entry authorization?
YES -> jump 1 , NO -> jump 1

5. 7 Are all entrances to the building, including emergency, equipment, and maintenance portals, controlled?
YES -> jump 1 , NO -> jump 21

5. 8 Are there multiple entrances to the BUILDING?
YES -> jump 1 , NO -> jump 5

5. 9 How many BUILDING entrances are there?
YES -> jump 1 , NO -> jump 1

5.10 How many BUILDING entrances are available to personnel access at all times?
YES -> jump 1 , NO -> jump 1

5.11 How many BUILDING entrances are available for personnel access only during normal working hours?
YES -> jump 1 , NO -> jump 1

5.12 How many BUILDING entrances are available for personnel access only during normal arrival or departure hours?
YES -> jump 1 , NO -> jump 1

5.13 Is BUILDING entry controlled DURING normal working hours?
YES -> jump 1 , NO -> jump 1

5.14 Is BUILDING entry controlled AFTER normal working hours?
YES -> jump 1 , NO -> jump 1

5.15 Is BUILDING entry controlled by a GUARD(s)?
YES -> jump 1 , NO -> jump 2

5.16 Does the guard permit BUILDING entry by a) visual recognition, b) verifying ID from a list, c) badge with no photo, d) badge with photo, e) other (specify)?
YES -> jump 1 , NO -> jump 1

5.17 Is BUILDING entry controlled by a KEY?
YES -> jump 1 , NO -> jump 3

5.18 How many persons have keys to the BUILDING?
YES -> jump 1 , NO -> jump 1

5.19 Is it difficult to duplicate BUILDING keys (ie, do keys have engraved instructions to prohibit their duplication, are they made on special blanks not available to others, etc.)?
YES -> jump 1 , NO -> jump 1

5.20 Is BUILDING entry controlled by a CIPHER LOCK(s)?
YES -> jump 1 , NO -> jump 3

5.21 How many persons have the combination to the BUILDING cipher lock(s)?
YES -> jump 1 , NO -> jump 1

5.22 Is the combination to the BUILDING cipher lock(s) changed on a regular basis?
YES -> jump 1 , NO -> jump 1

5.23 Is BUILDING entry controlled by MAGNETIC BADGE/CARD/KEY-CARD READERS?
YES -> jump 1 , NO -> jump 2

5.24 How many persons have magnetic cards, badges, or key cards permitting entry to the BUILDING?
YES -> jump 1 , NO -> jump 1

5.25 Are authorization lists and control mechanisms allowing BUILDING entry updated when a person's entry authority is revoked?
YES -> jump 1 , NO -> jump 2

5.26 When a person no longer is authorized for BUILDING entry, are a) authorization lists updated, b) locks/combinations changed, c) keys, badges, cards surrendered, d) other (specify).
YES -> jump 1 , NO -> jump 1

5.27 Is access to the BUILDING and to resources denied quickly enough to prevent damage to resources by a person who no longer has authorized access to the BUILDING?
YES -> jump 1 , NO -> jump 1

5.28 Do employes challenge persons in the BUILDING if they are not properly identifiable?
YES -> jump 1 , NO -> jump 1

5.29 Is there a control on badges, keys, combinations, and/or cards used for BUILDING entry?
YES -> jump 1 , NO -> jump 1

5.30 Are entries to or exits from the BUILDING by employes recorded at any time?
YES -> jump 1 , NO -> jump 5

5.31 How are employe BUILDING entries/exits recorded? a) magnetic key card, b) sign-in register, c) microprocessor, d) other (describe).
YES -> jump 1 , NO -> jump 1

5.32 Are BUILDING entries/exits by employes recorded DURING normal working hours?
YES -> jump 1 , NO -> jump 1

5.33 Are BUILDING entries/exits by employes recorded OUTSIDE OF normal working hours?
YES -> jump 1 , NO -> jump 1

5.34 Are BUILDING entries/exits by employes recorded during emergency situations?
YES -> jump 1 , NO -> jump 1

5.35 Are entries to or exits from the BUILDING by non-employes recorded at any time?
YES -> jump 1 , NO -> jump 5

5.36 How are non-employe BUILDING entries/exits recorded? a) magnetic key card, b) sign-in register, c) microprocessor, d) other (describe).
YES -> jump 1 , NO -> jump 1

5.37 Are BUILDING entries/exits by non-employes recorded DURING normal working hours?
YES -> jump 1 , NO -> jump 1

5.38 Are BUILDING entries/exits by non-employes recorded OUTSIDE OF of normal working hours?
YES -> jump 1 , NO -> jump 1

5.39 Are BUILDING entries/exits by non-employes recorded during emergency situations?
YES -> jump 1 , NO -> jump 1

5.40 Do BUILDING entrances have alarms and/or monitors (e.g., CCTV, guards, etc.)?
YES -> jump 1 , NO -> jump 9

5.41 Do all regularly-used BUILDING entrances have monitors and/or alarms?
YES -> jump 1 , NO -> jump 1

5.42 Do BUILDING emergency exits and other not-regularly-used operating entrances have monitors and/or alarms?
YES -> jump 1 , NO -> jump 1

5.43 Do BUILDING entrance/exit monitors transmit to a location where timely appropriate action will be taken?
YES -> jump 1 , NO -> jump 1

5.44 Do BUILDING entrance/exit monitors and/or alarms transmit to a) a main guard station off-site, b) a guard station in another building, c) a guard station in the same building, d) other (specify).
YES -> jump 1 , NO -> jump 1

5.45 Is a record from the BUILDING entrance/exit monitors and/or alarms kept in some form available for audit?
YES -> jump 1 , NO -> jump 1

5.46 Are there documented guidelines for evaluating appropriate responses to notifications from BUILDING entrance monitors and/or alarms?
YES -> jump 1 , NO -> jump 1

5.47 Are appropriate procedures for responding to a notification from BUILDING monitors and alarms defined and documented?
YES -> jump 1 , NO -> jump 1

5.48 Are personnel trained or drilled in how to respond to BUILDING monitors and alarms?
YES -> jump 1 , NO -> jump 1

5.49 Are the BUILDING's ground-level doors kept locked or guarded at all times?
YES -> jump 1 , NO -> jump 1

5.50 Does the building have exterior doors anywhere other than at ground level?
YES -> jump 1 , NO -> jump 2

5.51 Are the BUILDING's other-than-ground-level doors kept locked or otherwise controlled at all times?
YES -> jump 1 , NO -> jump 1

5.52 Does the BUILDING have windows?
YES -> jump 1 , NO -> jump 4

5.53 Are the BUILDING's windows kept locked or else barred or screened with a material that would prevent intrusion?
YES -> jump 1 , NO -> jump 1

5.54 Are BUILDING windows made of material that resists breaking and shattering?
YES -> jump 1 , NO -> jump 2

5.55 Has the fire department been alerted that BUILDING windows are made of material that resists breaking or shattering?
YES -> jump 1 , NO -> jump 1

Category 6 : COMMUNICATIONS

6. 1 Does the operating system ask the user to specify the earliest time for his next login?
YES -> jump 1 , NO -> jump 1

6. 2 Are separate, secure communications lines used for the computer?
YES -> jump 1 , NO -> jump 1

6. 3 Do the transmission (telephone) lines to the computer(s) pass through a switchboard?
YES -> jump 1 , NO -> jump 1

6. 4 Can the computer operator manually cut out an individual communication line?
YES -> jump 1 , NO -> jump 1

6. 5 Is there a way for a user to be certain that he is connected to the correct computer and not to a hostile one?
YES -> jump 1 , NO -> jump 1

6. 6 Is there error-detection and error-recovery hardware in place to deal with transmission errors?
YES -> jump 1 , NO -> jump 1

6. 7 Are transmission lines checked for bugging, wire-tapping, or illegal connections of pirate terminals?
YES -> jump 1 , NO -> jump 1

6. 8 Can the computer(s) be accessed by telephone?
YES -> jump 1 , NO -> jump 5

6. 9 Is information transmitted over the telephone encrypted?
YES -> jump 1 , NO -> jump 1

6.10 Is there a port-protection device in use at the computer center?
YES -> jump 1 , NO -> jump 3

6.11 Does the port-protection device camouflage the computer port from the user of an autodial modem?
YES -> jump 1 , NO -> jump 1

6.12 Can the port-protection device verify the user's telephone number and call the user back?
YES -> jump 1 , NO -> jump 1

Category 7 : COMPUTER OPERATING SYSTEM

7. 1 Does the operating system have a user-authentication process?
YES -> jump 1 , NO -> jump 5

7. 2 Does the operating system require a user (account) identification name or number to grant access to the system?
YES -> jump 1 , NO -> jump 1

7. 3 Does the operating system require a user (account) password to grant access to the system?
YES -> jump 1 , NO -> jump 1

7. 4 Does the operating system require an identification number for remote terminals to grant access to the system?
YES -> jump 1 , NO -> jump 1

7. 5 Does the operating system require a security classification to grant access to the system?
YES -> jump 1 , NO -> jump 1

7. 6 Are there controls governing job entry for batch, remote-entry, and on-line processing?
YES -> jump 1 , NO -> jump 1

7. 7 Is there a protection scheme for information in the system tables?
YES -> jump 1 , NO -> jump 1

7. 8 Are there hardware methods known to the data center staff for evading operational system security mechanisms (hardware "trap doors") in the computer system?
YES -> jump 1 , NO -> jump 3

7. 9 Are there hardware trap doors for evading operational system security mechanisms that are generally or publicly known (eg, they appear on hacker bulletin boards)?
YES -> jump 1 , NO -> jump 1

7.10 How many people (both employes and other persons) might be able to use the hardware trap doors (estimate)?
YES -> jump 1 , NO -> jump 1

7.11 Are there software methods known to data center staff that can evade operational system security mechanisms (software "trap doors") in the computer system?
YES -> jump 1 , NO -> jump 3

7.12 Are the software trap doors for evading operational system security mechanisms generally or publicly known (eg, appear on hacker bulletin boards, etc)?
YES -> jump 1 , NO -> jump 1

7.13 How many people (both employes and other persons) might be able to use the software trap doors (estimate)?
YES -> jump 1 , NO -> jump 1

7.14 Is the operating system stored in read-only memory?
YES -> jump 1 , NO -> jump 1

7.15 Are checks of operating-system integrity made periodically at a frequency determined by site management?
YES -> jump 1 , NO -> jump 1

7.16 Are defensive or diversionary actions taken by the operating system for certain violations?
YES -> jump 1 , NO -> jump 10

7.17 Does the operating system disable the communications channel in response to repeated system-access violations?
YES -> jump 1 , NO -> jump 1

7.18 Does the operating system generate an automatic logoff for terminal inactivity?
YES -> jump 1 , NO -> jump 1

7.19 Does the operating system suspend or cancel program execution for inappropriate (unauthorized, ill-conceived, poorly thought out, or stupid) program action?
YES -> jump 1 , NO -> jump 2

7.20 Does the operating system log (or otherwise record) and suspend program activity for attempts to access an unauthorized file?
YES -> jump 1 , NO -> jump 1

7.21 Does the operating system log (or otherwise record) and suspend program activity for violations of file-access privilege (R,W,E,M,D) in an otherwise authorized file?
YES -> jump 1 , NO -> jump 1

7.22 Does the operating system take defensive or diversionary action in response to unauthorized security-table access attempts?
YES -> jump 1 , NO -> jump 2

7.23 What action does the operating system take for unauthorized security-table access attempts? a) disconnects user/terminal, b) causes automatic logoff, c) sounds alarm, d) posts to log, e) other.
YES -> jump 1 , NO -> jump 1

7.24 Does the operating system consolidate session statistics to detect a generally high frequency of violations?
YES -> jump 1 , NO -> jump 1

7.25 Are ALL violations and attempted violations of protected files recorded?
YES -> jump 1 , NO -> jump 1

Category 8 : COMPUTER OPERATIONS

8. 1 Can computer operators make programming or processing modifications from the operations console?
YES -> jump 1 , NO -> jump 1

8. 2 Are logs kept of hardware malfunctions?
YES -> jump 1 , NO -> jump 1

8. 3 Do operators check "read-only" storage media to make sure that they cannot be written to?
YES -> jump 1 , NO -> jump 1

8. 4 Is there a documented standard operating procedure (SOP) for the physical destruction of sensitive and/or classified waste?
YES -> jump 1 , NO -> jump 1

8. 5 Are waste magnetic media that contain sensitive or classified information disposed of as sensitive waste in a manner commensurate with their sensitivity?
YES -> jump 1 , NO -> jump 1

8. 6 Are all residual files destroyed at the completion or abortion of a job?
YES -> jump 1 , NO -> jump 1

8. 7 Are all forms of sensitive or classified waste protected at a level commensurate with its sensitivity until it can be destroyed?
YES -> jump 1 , NO -> jump 5

8. 8 Are sensitive or classified waste printouts and forms shredded, burned, or otherwise destroyed?
YES -> jump 1 , NO -> jump 1

8. 9 Are printer ribbons used for sensitive or classified output destroyed?
YES -> jump 1 , NO -> jump 1

8.10 Are the carbons used to print multiple forms for sensitive or classified applications destroyed?
YES -> jump 1 , NO -> jump 1

8.11 Are waste punched cards used in sensitive or classified applications destroyed?
YES -> jump 1 , NO -> jump 1

8.12 Is the waste output from partially-completed jobs that have been restarted treated with the same level of security as "good" jobs would be?
YES -> jump 1 , NO -> jump 1

8.13 Is output clearly marked and controlled to ensure its delivery to the authorized recipient?
YES -> jump 1 , NO -> jump 1

8.14 Is output clearly marked to indicate its level of classification and sensitivity (and hence its required level of protection)?
YES -> jump 1 , NO -> jump 1

8.15 Do computer operations personnel protect reports and output containing sensitive, official use only, or classified information from casual browsing and other unauthorized use?
YES -> jump 1 , NO -> jump 1

8.16 Are expiration dates assigned to user files automatically?
YES -> jump 1 , NO -> jump 1

8.17 Does computer operations have the responsibility for automatic release of outdated user files?
YES -> jump 1 , NO -> jump 1

8.18 Are released user files overwritten instead of just having their directory addresses removed?
YES -> jump 1 , NO -> jump 2

8.19 Are released user files overwritten a) by hardware or b) by software?
YES -> jump 1 , NO -> jump 1

8.20 Does computer operations have the responsibility for automatic user-file backup when system backups are done?
YES -> jump 1 , NO -> jump 1

Category 9 : COMPUTER ROOM CONSTRUCTION

9. 1 Is the computer equipment and associated equipment housed in a separate dedicated ROOM(s) within the BUILDING?
YES -> jump 1 , NO -> jump 1

9. 2 Does a barrier separate the computer ROOM from the rest of the BUILDING?
YES -> jump 1 , NO -> jump 7

9. 3 What best describes the ROOM-barrier's construction: a) concrete, concrete block, etc., b) standard walls, c) chain-link fence, d) attached partial walls, e) movable walls, f) other.
YES -> jump 1 , NO -> jump 1

9. 4 Is the barrier separating the computer ROOM from the rest of the BUILDING a fire wall?
YES -> jump 1 , NO -> jump 1

9. 5 The construction of the computer-ROOM doors/gates is: a) vault doors, b) metal/ metal clad, c) solid wood, d) hollow-core wood, e) glass, f) wood/metal & glass, g) openwork metal, h) other (specify).
YES -> jump 1 , NO -> jump 1

9. 6 Do computer-ROOM doors or gates fit flush into the framework?
YES -> jump 1 , NO -> jump 1

9. 7 Do computer-ROOM doors or gates have a large open space above them, as in a "Dutch" door?
YES -> jump 1 , NO -> jump 1

9. 8 How many entrances to the computer ROOM are there?
YES -> jump 1 , NO -> jump 1

9. 9 Are there EXTERIOR doors, windows, or entryways that give direct visual or physical access to the computer ROOM from outside the building?
YES -> jump 1 , NO -> jump 7

9.10 Are the EXTERIOR doors, windows, and entryways leading into the computer ROOM watertight?
YES -> jump 1 , NO -> jump 1

9.11 Does the computer ROOM have EXTERIOR windows?
YES -> jump 1 , NO -> jump 5

9.12 Do EXTERIOR computer ROOM windows provide a view of computer operations from outside the building?
YES -> jump 1 , NO -> jump 4

9.13 Are EXTERIOR computer ROOM windows barred or screened with heavy metal mesh?
YES -> jump 1 , NO -> jump 1

9.14 Are EXTERIOR computer ROOM windows large plateglass windows?
YES -> jump 1 , NO -> jump 1

9.15 Do EXTERIOR computer ROOM windows contain embedded wire support to mitigate shattering?
YES -> jump 1 , NO -> jump 1

9.16 Does the computer ROOM have INTERIOR windows?
YES -> jump 1 , NO -> jump 7

9.17 Do INTERIOR computer ROOM windows provide a view of computer operations from the surrounding area within the building?
YES -> jump 1 , NO -> jump 1

9.18 Are INTERIOR computer ROOM windows barred or screened with heavy metal mesh?
YES -> jump 1 , NO -> jump 1

9.19 Are INTERIOR computer ROOM windows large plateglass windows?
YES -> jump 1 , NO -> jump 1

9.20 Do INTERIOR computer ROOM windows contain embedded wire support to mitigate shattering?
YES -> jump 1 , NO -> jump 1

9.21 Are any INTERIOR computer room windows used as pass-throughs (such a: for distributing output or accepting input)?
YES -> jump 1 , NO -> jump 2

9.22 Are INTERIOR computer ROOM windows that are used as pass-throughs kept locked or otherwise controlled when not in use?
YES -> jump 1 , NO -> jump 1

9.23 Has the structural flooring in the computer ROOM adequate strength t(support both the total and the local loads that will be imposed by the various items of equipment?
YES -> jump 1 , NO -> jump 1

9.24 Is there equipment available in the computer ROOM to exhaust smoke and combustion products directly to the atmosphere after a fire?
YES -> jump 1 , NO -> jump 1

9.25 Are all computer ROOM electrical cables and wiring located away from normal traffic paths or protected from being disturbed by traffic?
YES -> jump 1 , NO -> jump 1

9.26 Are all cables entering and exiting the computer ROOM clearly marked and uniquely identified?
YES -> jump 1 , NO -> jump 1

9.27 Have OVERHEAD steam or water pipes (except sprinklers) been eliminated from the computer ROOM?
YES -> jump 1 , NO -> jump 1

9.28 Are pipe and wire penetrations into the computer ROOM watertight?
YES -> jump 1 , NO -> jump 1

9.29 Is there drainage in the computer ROOM?
YES -> jump 1 , NO -> jump 3

9.30 Is the drainage from the computer ROOM sufficient to prevent water overflow from adjacent areas?
YES -> jump 1 , NO -> jump 1

9.31 Are floor drains in the computer ROOM fitted with anti-backflow valves?
YES -> jump 1 , NO -> jump 1

9.32 Is the structural ceiling of the computer ROOM constructed to conduct water from higher levels away from all hardware?
YES -> jump 1 , NO -> jump 1

Category 10 : COMPUTER ROOM CONTENTS

10. 1 Are there curtains and/or drapes in the computer ROOM?
YES -> jump 1 , NO -> jump 2

10. 2 Are computer ROOM curtains or drapes made of non-combustible or fire-resistant materials?
YES -> jump 1 , NO -> jump 1

10. 3 Is there furniture in the computer ROOM?
YES -> jump 1 , NO -> jump 2

10. 4 Are computer ROOM chairs and other furniture made of non-combustible or fire-resistant materials?
YES -> jump 1 , NO -> jump 1

10. 5 Are there loose rugs or mats in the computer ROOM?
YES -> jump 1 , NO -> jump 3

10. 6 Are computer ROOM loose rugs or mats made of non-combustible or fire-resistant materials?
YES -> jump 1 , NO -> jump 1

10. 7 Are computer ROOM loose rugs and mats kept free of dirt and dust?
YES -> jump 1 , NO -> jump 1

10. 8 Does the computer ROOM have either installed carpeting (as opposed to loose rugs) or carpeted floor tiles?
YES -> jump 1 , NO -> jump 6

10. 9 Is the computer ROOM carpeting made of anti-static material or treated regularly to prevent damage to equipment from static discharge?
YES -> jump 1 , NO -> jump 1

10.10 Is the computer ROOM carpeting cleaned on a regular basis?
YES -> jump 1 , NO -> jump 3

10.11 Is the computer ROOM carpeting vacuumed frequently?
YES -> jump 1 , NO -> jump 1

10.12 Is the computer ROOM carpeting shampooed at least yearly?
YES -> jump 1 , NO -> jump 1

10.13 Is the computer ROOM carpeting made of fire-resistant material?
YES -> jump 1 , NO -> jump 1

10.14 Are waste containers used in the computer ROOM?
YES -> jump 1 , NO -> jump 5

10.15 Are computer ROOM waste containers considered to be low-fire-hazard containers?
YES -> jump 1 , NO -> jump 1

10.16 Do computer ROOM waste containers have metal lids?
YES -> jump 1 , NO -> jump 1

10.17 Are computer ROOM waste containers emptied often enough to prevent large waste accumulations or overflow?
YES -> jump 1 , NO -> jump 1

10.18 Are computer ROOM waste containers emptied outside the computer ROOM to reduce dust discharge?
YES -> jump 1 , NO -> jump 1

10.19 Is paper-bursting equipment, paper-shredding equipment, or report distribution forms-handling equipment permitted in the computer ROOM?
YES -> jump 1 , NO -> jump 1

10.20 Are any paper products and supplies kept or stored in the computer ROOM? (if yes, additional questions will be asked to sort out the specifics)
YES -> jump 1 , NO -> jump 6

10.21 Is more than one day's requirement of paper and stationery supplies stored inside the computer ROOM?
YES -> jump 1 , NO -> jump 4

10.22 What is the approximate quantity of paper products in the computer ROOM (cu. ft.)?
YES -> jump 1 , NO -> jump 1

10.23 Are paper and stationery supplies that are stored in the computer ROOM left in closed boxes until needed?
YES -> jump 1 , NO -> jump 1

10.24 Are paper and other supplies that are stored in the computer ROOM kept in a water-free/water-resistant location?
YES -> jump 1 , NO -> jump 1

10.25 Are empty supply boxes and waste paper removed frequently on a scheduled basis from the computer ROOM?
YES -> jump 1 , NO -> jump 1

10.26 Is an industrial wet/dry vacuum cleaner available for timely use at the data center?
YES -> jump 1 , NO -> jump 1

10.27 Are there waterproof sheets or covers available in the computer ROOM for use if there is overhead water leakage or discharge?
YES -> jump 1 , NO -> jump 3

10.28 Are the waterproof sheets or covers in the computer ROOM large enough and numerous enough to cover all hardware, equipment, and supplies that could damaged by water?
YES -> jump 1 , NO -> jump 1

10.29 Are waterproof sheets and/or covers easily accessible and so located that the hardware, equipment, and/or supplies can be covered quickly?
YES -> jump 1 , NO -> jump 1

10.30 Are caustic or flammable cleaning agents permitted in the computer ROOM?
YES -> jump 1 , NO -> jump 3

10.31 Is the amount of the caustic or flammable cleaning agents that are in the computer ROOM more than the amount required to perform one day's work?
YES -> jump 1 , NO -> jump 1

10.32 Are the caustic or flammable cleaning agents that are in the computer ROOM kept in approved containers?
YES -> jump 1 , NO -> jump 1

10.33 In the computer ROOM, is there a certified-fireproof safe or cabinet, specifically designed for low-temperature magnetic media, in which to store critical documents, tapes, and files?
YES -> jump 1 , NO -> jump 1

Category 11 : COMPUTER ROOM ENTRY

11. 1 Are computer ROOM doors and gates kept locked or otherwise controlled at ANY time?
YES -> jump 1 , NO -> jump 10

11. 2 Are computer ROOM doors locked or otherwise controlled DURING normal working hours?
YES -> jump 1 , NO -> jump 1

11. 3 Are computer ROOM doors locked or otherwise controlled OUTSIDE OF normal working hours?
YES -> jump 1 , NO -> jump 1

11. 4 Are computer ROOM doors locked or otherwise controlled DURING EMERGENCY situations?
YES -> jump 1 , NO -> jump 1

11. 5 Are computer ROOM doors and gates checked periodically to see that they are locked?
YES -> jump 1 , NO -> jump 2

11. 6 How often is it verified that computer ROOM doors or gates are locked?
YES -> jump 1 , NO -> jump 1

11. 7 Is someone responsible for verifying that computer ROOM doors or gates are locked?
YES -> jump 1 , NO -> jump 2

11. 8 Who is responsible for verifying locked computer ROOM doors? a) computer operations, b) building security, c) site security, d) municipal police, e) hired off-site security, f) other.
YES -> jump 1 , NO -> jump 1

11. 9 Is corrective action taken if a computer ROOM door or gate is found unsecured?
YES -> jump 1 , NO -> jump 2

11.10 What happens if a computer ROOM door or gate is found unlocked? a) security notified, b) police notified, c) building security notified, d) locked by finder, e) documented in written report, f)other.
YES -> jump 1 , NO -> jump 1

11.11 Is entry to the computer ROOM controlled at ANY time?
YES -> jump 1 , NO -> jump 43

11.12 Is computer ROOM entry controlled DURING normal working hours?
YES -> jump 1 , NO -> jump 1

11.13 Is computer ROOM entry controlled OUTSIDE OF normal working hours?
YES -> jump 1 , NO -> jump 1

11.14 Is computer ROOM entry controlled DURING EMERGENCY situations?
YES -> jump 1 , NO -> jump 1

11.15 Is computer ROOM entry controlled when the computer is unattended?
YES -> jump 1 , NO -> jump 1

11.16 Is computer ROOM entry controlled (either entirely or in part) by a GUARD(s) or other individual?
YES -> jump 1 , NO -> jump 2

11.17 Does the guard or other individual permit computer ROOM entry by a) visual recognition, b) verifying ID from a list, c) badge with no photo, d) badge with photo, e) other.
YES -> jump 1 , NO -> jump 1

11.18 Is computer ROOM entry controlled (either entirely or in part) by a KEY?
YES -> jump 1 , NO -> jump 3

11.19 How many persons have keys to the computer ROOM(s)?
YES -> jump 1 , NO -> jump 1

11.20 Is it difficult to duplicate keys to the computer ROOM (ie, do keys have engraved instructions prohibiting duplication, are they on non-standard blanks, etc)?
YES -> jump 1 , NO -> jump 1

11.21 Is computer ROOM entry controlled (either entirely or in part) by a CIPHER LOCK?
YES -> jump 1 , NO -> jump 4

11.22 How many persons know the combination to the computer ROOM cipher lock(s)?
YES -> jump 1 , NO -> jump 1

11.23 Is the combination to computer ROOM cipher locks changed in a time frame commensurate with the sensitivity of the data processing being done?
YES -> jump 1 , NO -> jump 1

11.24 Are personnel instructed to conceal cipher lock combinations and operations from the view of others?
YES -> jump 1 , NO -> jump 1

11.25 Is computer ROOM entry controlled by a MAGNETIC BADGE/CARD READER?
YES -> jump 1 , NO -> jump 2

11.26 How many persons have magnetic badges or cards permitting computer ROOM entry?
YES -> jump 1 , NO -> jump 1

11.27 Are security personnel notified of employes permitted entry to the computer ROOM outside of normal working hours?
YES -> jump 1 , NO -> jump 1

11.28 Does the computer ROOM have doors/portals designated solely for emergency use (ie, emergency exits)?
YES -> jump 1 , NO -> jump 5

11.29 Can computer ROOM emergency exits be operated from outside the computer room?
YES -> jump 1 , NO -> jump 1

11.30 Is the status of ALL emergency exits from the computer ROOM monitored (e.g., by CCTV, guards, operations staff)?
YES -> jump 1 , NO -> jump 2

11.31 How are the emergency exits from the computer ROOM monitored (by CCTV, guards, operations staff, other)?
YES -> jump 1 , NO -> jump 1

11.32 Are there alarms on ALL emergency exits from the computer ROOM?
YES -> jump 1 , NO -> jump 1

11.33 Would access to the computer ROOM still be controlled in case of fire or other emergency or disaster?
YES -> jump 1 , NO -> jump 1

11.34 Are custodial personnel permitted entry to the computer ROOM when it is unattended?
YES -> jump 1 , NO -> jump 1

11.35 Are physical-security personnel permitted entry to the computer ROOM when it is unattended?
YES -> jump 1 , NO -> jump 1

11.36 Are there effective procedures for authorizing computer ROOM entry?
YES -> jump 1 , NO -> jump 1

11.37 Is someone responsible for authorizing computer ROOM entry?
YES -> jump 1 , NO -> jump 2

11.38 Indicate who is responsible for authorizing computer ROOM entry: a) system manager, b) system security officer, c) building security office, d) site security office, e) other.
YES -> jump 1 , NO -> jump 1

11.39 Is there a procedure to control badges, keys, combinations, and/or cards used for entry to the computer ROOM?
YES -> jump 1 , NO -> jump 2

11.40 What is the procedure for controlling badges, keys, combinations, and/or cards used for entry to the computer ROOM?
YES -> jump 1 , NO -> jump 1

11.41 Are authorization lists and control mechanisms allowing entry into the computer ROOM updated when a person's authorization for entry has been revoked?
YES -> jump 1 , NO -> jump 2

11.42 When an individual's computer ROOM entry authority is revoked, are a) authorization lists revised, b) locks/combinations changed, c) badges, keys, cards surrendered, d) other.
YES -> jump 1 , NO -> jump 1

11.43 Is access to computer ROOM resources denied quickly enough to prevent damage to the resources by a person whose computer ROOM entry authorization has been revoked?
YES -> jump 1 , NO -> jump 1

11.44 Are entries to the computer ROOM by employes other than the assigned operations staff recorded?
YES -> jump 1 , NO -> jump 5

11.45 Are entries to the computer ROOM by employes other than the assigned operations staff recorded DURING normal working hours?
YES -> jump 1 , NO -> jump 1

11.46 Are computer-ROOM entries by employes other than the assigned operations staff recorded OUTSIDE OF normal working hours?
YES -> jump 1 , NO -> jump 1

11.47 Are computer-ROOM entries by employes others than assigned operations staff recorded DURING EMERGENCY situations?
YES -> jump 1 , NO -> jump 1

11.48 By what means are employe (except operations staff) computer-ROOM entries recorded? a) magnetic key card, b) sign-in register, c) other.
YES -> jump 1 , NO -> jump 1

11.49 Are entries to the computer ROOM by non-employes recorded?
YES -> jump 1 , NO -> jump 5

11.50 Are entries to the computer ROOM by non-employes recorded DURING normal working hours?
YES -> jump 1 , NO -> jump 1

11.51 Are computer ROOM entries by non-employes recorded OUTSIDE OF normal working hours?
YES -> jump 1 , NO -> jump 1

11.52 Are computer ROOM entries by non-employes recorded DURING EMERGENCY situations?
YES -> jump 1 , NO -> jump 1

11.53 By what means are non-employes' computer ROOM entries recorded? a) magnetic key card, b) sign-in register, c) other.
YES -> jump 1 , NO -> jump 1

11.54 Do employes challenge persons in the computer ROOM if the persons are not properly identifiable?
YES -> jump 1 , NO -> jump 1

Category 12 : COMPUTER ROOM PROCEDURES & POLICY

12. 1 Are there authorization lists for who may use, operate, and perform maintenance on computer equipment?
YES -> jump 1 , NO -> jump 9

12. 2 Who is responsible for authorizing access to the computer? a) system manager, b) system security officer, c) system operator, d) other.
YES -> jump 1 , NO -> jump 1

12. 3 Is there an authorization list for who may USE the computer?
YES -> jump 1 , NO -> jump 1

12. 4 Is there an authorization list for who may OPERATE the computer?
YES -> jump 1 , NO -> jump 1

12. 5 Is there an authorization list for who may MAINTAIN computer equipment?
YES -> jump 1 , NO -> jump 1

12. 6 Are authorization lists for using, operating, and maintaining computer equipment updated when a person's authorization is revoked?
YES -> jump 1 , NO -> jump 2

12. 7 What happens when computer use, etc, authorizations are revoked: a) authorization lists revised, b) locks and/or combinations changed, c) keys/cards/badges surrendered, d) other.
YES -> jump 1 , NO -> jump 1

12. 8 Are backups of current authorization lists for computer use, operation, and maintenance kept at an off-site location?
YES -> jump 1 , NO -> jump 1

12. 9 Is access to computer equipment denied quickly enough to prevent damage to the equipment by a person whose use/operation/maintenance authorization has been revoked?
YES -> jump 1 , NO -> jump 1

12.10 Are there authorization lists to use, modify, maintain, or update system and system applications software?
YES -> jump 1 , NO -> jump 9

12.11 Is there an authorization list for who may MAINTAIN OR ALTER SYSTEM SOFTWARE?
YES -> jump 1 , NO -> jump 1

12.12 Is there an authorization list for who may MAINTAIN OR MODIFY system APPLICATIONS PROGRAMS AND DATA FILES?
YES -> jump 1 , NO -> jump 1

12.13 Is there an authorization list for who may USE SYSTEM SOFTWARE?
YES -> jump 1 , NO -> jump 1

12.14 Is there an authorization list for who may USE system APPLICATIONS PROGRAMS AND DATA FILES?
YES -> jump 1 , NO -> jump 1

12.15 Are authorization lists for who may use, modify, maintain, or update system and system applications software updated when a person's authorization is revoked?
YES -> jump 1 , NO -> jump 2

12.16 What happens if authorizations for system software use,etc are revoked: are a) authorization lists revised, b) locks and/or combinations changed, c) keys/cards/badges surrendered, d) other.
YES -> jump 1 , NO -> jump 1

12.17 Is access to system software, applications, and data files denied quickly enough to prevent damage to them by a person whose use, etc. authorization has been revoked?
YES -> jump 1 , NO -> jump 1

12.18 Are backups of current authorization lists of who may use, modify, or update system software, data, and applications programs kept at an off-site location?
YES -> jump 1 , NO -> jump 1

12.19 Are there authorization lists to use, modify, or update computer-related documents?
YES -> jump 1 , NO -> jump 8

12.20 Is there an authorization list for who may USE computer-related documents?
YES -> jump 1 , NO -> jump 1

12.21 Is there an authorization list for who may MODIFY computer-related documents (input sheets, reports, documentation, output, program listings, etc.)
YES -> jump 1 , NO -> jump 1

12.22 Is there an authorization list for who may UPDATE computer-related documents (input sheets, reports, manuals, output, program listings)?
YES -> jump 1 , NO -> jump 1

12.23 Are authorization lists for who may use, modify, and update computer-related documents updated when a person's authorization is revoked?
YES -> jump 1 , NO -> jump 2

12.24 What happens when authorizations to use,etc documents are revoked: a) authorization lists revised, b) locks and/or combinations changed, c) keys/cards/badges surrendered, d) other.
YES -> jump 1 , NO -> jump 1

12.25 Is access to computer-related documents denied quickly enough to prevent damage to them by a person whose use, modification, and updating authorization has been revoked?
YES -> jump 1 , NO -> jump 1

12.26 Is a backup of the current authorization list for who may use, modify, or update computer-related documents kept in an off-site location?
YES -> jump 1 , NO -> jump 1

12.27 Is there an authorization list for who may request and use system dumps?
YES -> jump 1 , NO -> jump 5

12.28 Is the authorization list for who may request and use system dumps updated to when a person's authorization is revoked?
YES -> jump 1 , NO -> jump 2

12.29 What happens when system-dump authorization is revoked: a) authorization lists revised, b) locks and/or combinations changed, c) keys/cards/badges surrendered, d) other.
YES -> jump 1 , NO -> jump 1

12.30 Is access to system dumps denied quickly enough to prevent damage to computing resources by a person whose system-dump access authorization has been revoked?
YES -> jump 1 , NO -> jump 1

12.31 Are backup copies of current authorization lists of who may request and use system dumps kept at an off-site location?
YES -> jump 1 , NO -> jump 1

12.32 Are output devices, monitors, and displays positioned to prevent unauthorized personnel from seeing or otherwise acquiring the information from computer output?
YES -> jump 1 , NO -> jump 1

12.33 Are there enforced procedures to control the removal of storage media and devices, computer equipment and parts, and documents from the computer ROOM?
YES -> jump 1 , NO -> jump 4

12.34 Are there enforced procedures to control the removal of STORAGE MEDIA AND STORAGE DEVICES from the computer ROOM?
YES -> jump 1 , NO -> jump 1

12.35 Are there enforced procedures to control the removal of computer equipment and parts from the computer ROOM?
YES -> jump 1 , NO -> jump 1

12.36 Are there enforced procedures to control the removal of documents (input or data listings, output, program listings, reports, manuals, etc.) from the computer ROOM?
YES -> jump 1 , NO -> jump 1

12.37 Are hardware protective and security features (e.g., locks, surge protectors, port protection devices, etc.) checked regularly to see that they are functioning as intended?
YES -> jump 1 , NO -> jump 1

12.38 Is the integrity of the hardware protective features tested at a frequency determined by facility management?
YES -> jump 1 , NO -> jump 1

12.39 Is smoking permitted in the computer ROOM?
YES -> jump 1 , NO -> jump 1

12.40 Are beverages or food permitted in the computer ROOM?
YES -> jump 1 , NO -> jump 1

12.41 Are potted plants or vases of fresh flowers permitted in the computer ROOM?
YES -> jump 1 , NO -> jump 1

12.42 Is the computer ROOM inspected regularly for neatness and cleanliness?
YES -> jump 1 , NO -> jump 1

12.43 Are work areas in the computer ROOM monitored for unauthorized use?
YES -> jump 1 , NO -> jump 1

Category 13 : COMPUTER ROOM RAISED FLOOR

13. 1 Does the computer ROOM have a raised floor?
YES -> jump 1 , NO -> jump 28

13. 2 Has the raised floor in the computer ROOM adequate strength to support both the total and the local loads that will be imposed by the various items of equipment?
YES -> jump 1 , NO -> jump 1

13. 3 Is there space for a person to crawl UNDER the floor in the computer ROOM?
YES -> jump 1 , NO -> jump 2

13. 4 Is the area UNDER the computer ROOM floor blocked to restrict entry from outside the computer ROOM?
YES -> jump 1 , NO -> jump 1

13. 5 Are floor tile removers available in the computer ROOM near operations personnel?
YES -> jump 1 , NO -> jump 1

13. 6 Are the locations of floor tile removers clearly marked and visible above equipment?
YES -> jump 1 , NO -> jump 1

13. 7 Is the computer ROOM structural floor made of concrete or other combustion-retardant material?
YES -> jump 1 , NO -> jump 1

13. 8 Is the raised flooring and flooring supports in the computer ROOM made of combustion-retardant material?
YES -> jump 1 , NO -> jump 1

13. 9 Is the space UNDER the computer ROOM floor blocked to inhibit smoke and fire infiltration to and from adjacent areas such as store rooms, media vaults, and communications closets?
YES -> jump 1 , NO -> jump 1

13.10 Is the space UNDER the raised floor in the computer ROOM used for storage of paper and/or other combustibles (Class A materials)?
YES -> jump 1 , NO -> jump 1

13.11 Are smoke/fire detectors installed UNDER the raised floor in the computer ROOM?
YES -> jump 1 , NO -> jump 2

13.12 Are UNDER-FLOOR smoke-detector heads identified by markers that are clearly visible to computer room personnel?
YES -> jump 1 , NO -> jump 1

13.13 Is there an automatic fire-protection (sprinkler) system installed UNDER the raised floor in the computer ROOM?
YES -> jump 1 , NO -> jump 5

13.14 Is water the extinguishing agent for the automatic fire-protection system UNDER the computer ROOM raised floor?
YES -> jump 3 , NO -> jump 1

13.15 What is the extinguishing agent for the automatic fire-protection system UNDER the computer ROOM raised floor? a) Halon, b) CO2, c) foam, d) other.
YES -> jump 1 , NO -> jump 1

13.16 What is the quantity of the extinguishing agent (lbs.) for the automatic fire-protection system UNDER the computer ROOM raised floor?
YES -> jump 1 , NO -> jump 1

13.17 Is there either a continuous supply or a backup supply of the extinguishing agent for the automatic fire-protection system UNDER the computer ROOM raised floor somewhere nearby?
YES -> jump 1 , NO -> jump 1

13.18 Is drainage UNDER the raised floor in the computer ROOM sufficient to remove accumulated liquid quickly?
YES -> jump 1 , NO -> jump 1

13.19 Are sensors installed to detect water accumulation UNDER the raised floor in the computer ROOM?
YES -> jump 1 , NO -> jump 1

13.20 Are there electrical outlets UNDER the raised floor in the computer ROOM?
YES -> jump 1 , NO -> jump 2

13.21 Are all electrical outlets and connectors UNDER the raised floor in the computer ROOM watertight?
YES -> jump 1 , NO -> jump 1

13.22 Are there cables and/or wiring UNDER the raised floor in the computer ROOM?
YES -> jump 1 , NO -> jump 4

13.23 Are all cables and wiring in the computer ROOM located UNDER the raised floor?
YES -> jump 1 , NO -> jump 1

13.24 Are all cables and wiring UNDER the raised floor in the computer ROOM watertight or otherwise protected from water damage?
YES -> jump 1 , NO -> jump 1

13.25 Are ALL cables under the raised floor clearly marked and uniquely identified?
YES -> jump 1 , NO -> jump 1

13.26 Is all computer ROOM equipment installed ON or ABOVE the raised floor?
YES -> jump 1 , NO -> jump 1

13.27 Is the UNDER floor area beneath the computer ROOM raised floor kept clean of dust and dirt?
YES -> jump 1 , NO -> jump 1

13.28 How often is the UNDER-floor area beneath the computer ROOM raised floor cleaned?
YES -> jump 1 , NO -> jump 1

Category 14 : COMPUTER ROOM SENSORS & ALARMS

14. 1 Are there surveillance monitors (e.g., CCTV), intrusion sensors, or alarms for the computer ROOM ENTRANCES?
YES -> jump 1 , NO -> jump 7

14. 2 Do surveillance monitors, intrusion sensors, or alarms operate for normal operating computer ROOM entrances?
YES -> jump 1 , NO -> jump 1

14. 3 Do surveillance monitors, intrusion sensors, or alarms operate for emergency exits and emergency situations in the computer ROOM?
YES -> jump 1 , NO -> jump 1

14. 4 Do surveillance monitors, intrusion sensors, or alarms operate for non-normal computer ROOM entrances, such as delivery portals?
YES -> jump 1 , NO -> jump 1

14. 5 Do computer ROOM entrance monitors, sensors, and/or alarms transmit to a location where timely action will be taken?
YES -> jump 1 , NO -> jump 2

14. 6 To where do the computer ROOM entrance monitors, etc., transmit? a) main security station off-site, b) security station in different building, c) security station in same building, d) other (specify).
YES -> jump 1 , NO -> jump 1

14. 7 Are records from the computer ROOM entrance surveillance monitors, intrusion sensors, and/or alarms kept in some form available for audit?
YES -> jump 1 , NO -> jump 1

14. 8 Are surveillance or sensor devices used WITHIN the computer ROOM (this is separate from AND/OR in addition to any such devices used for computer ROOM ENTRANCES) ?
YES -> jump 1 , NO -> jump 4

14. 9 Which surveillance or sensor devices are used in the computer ROOM: a) door switches, b) motion detectors, c) breakwire sensors, d) vibration sensors, e) closed-circuit TV, f) other (specify).
YES -> jump 1 , NO -> jump 1

14.10 Is output from the computer ROOM surveillance or sensor devices transmitted outside the computer room?
YES -> jump 1 , NO -> jump 2

14.11 Where do the computer ROOM surveillance and/or sensor devices transmit: a) security station off-site, b) security station, different building, c) security station, same building, d) other (specify).
YES -> jump 1 , NO -> jump 1

14.12 Is smoke/fire DETECTION equipment installed in the computer ROOM?
YES -> jump 1 , NO -> jump 6

14.13 Does the smoke/fire DETECTION system in the computer ROOM automatically either shut down or reverse the ventilation air flow?
YES -> jump 1 , NO -> jump 1

14.14 Does the smoke/fire DETECTION system in the computer ROOM automatically shut down power to the computer system?
YES -> jump 1 , NO -> jump 1

14.15 Does the computer ROOM smoke/fire DETECTION system shut down computer ROOM heating?
YES -> jump 1 , NO -> jump 1

14.16 Is the computer ROOM smoke/fire DETECTION system serviced and tested on a regularly scheduled basis?
YES -> jump 1 , NO -> jump 1

14.17 What devices are incorporated into the computer ROOM smoke/fire DETECTION system? a) ionization smoke detector, b) photoelectric smoke detector, c) heat rise detector, d) other (specify).
YES -> jump 1 , NO -> jump 1

14.18 Are smoke/fire DETECTORS installed inside computer ROOM equipment cabinets?
YES -> jump 1 , NO -> jump 1

14.19 Are there annunciator panels to assist in quickly locating hidden sources of fire or smoke in the computer ROOM?
YES -> jump 1 , NO -> jump 1

14.20 Is there a smoke/ fire ALARM system installed in the computer ROOM?
YES -> jump 1 , NO -> jump 5

14.21 Does the computer ROOM smoke/fire ALARM system report the specific location of the smoke or fire?
YES -> jump 1 , NO -> jump 1

14.22 Does the computer ROOM smoke/fire ALARM sound at other locations within the building as well as within the computer room?
YES -> jump 1 , NO -> jump 2

14.23 Where does the computer ROOM smoke/fire ALARM sound? a) the organization's main security station, b) municipal fire station, c) municipal police station, d) computer ROOM, e) other (specify).
YES -> jump 1 , NO -> jump 1

14.24 Is the computer ROOM smoke/fire ALARM system serviced and tested on a regularly scheduled basis?
YES -> jump 1 , NO -> jump 1

14.25 Are there effective and properly placed monitoring devices that generate a recorded history of temperature and humidity trends in the data center?
YES -> jump 1 , NO -> jump 1

Category 15 : COMPUTER ROOM SUSPENDED CEILING

15. 1 Does the computer ROOM have a suspended ceiling?
YES -> jump 1 , NO -> jump 14

15. 2 Is there a space large enough to hold a person between the suspended ceiling and the structural ceiling of the computer ROOM?
YES -> jump 1 , NO -> jump 4

15. 3 Is entry to the space between the suspended ceiling and the structural ceiling in the computer ROOM obvious to the casual observer?
YES -> jump 1 , NO -> jump 1

15. 4 Is entry to the space between the suspended ceiling and the structural ceiling in the computer ROOM controlled in some way?
YES -> jump 1 , NO -> jump 2

15. 5 How is entry to the space between the suspended ceiling and the structural ceiling in the computer ROOM controlled?
YES -> jump 1 , NO -> jump 1

15. 6 Are the computer ROOM walls extended above the suspended ceiling either to the structural ceiling or to the roof?
YES -> jump 1 , NO -> jump 1

15. 7 Is the tile in the computer ROOM's suspended ceiling made of non-combustible or high melting-point materials (including supports)?
YES -> jump 1 , NO -> jump 1

15. 8 Is a smoke/fire detector installed BETWEEN the suspended ceiling and the structural ceiling in the computer ROOM?
YES -> jump 1 , NO -> jump 1

15. 9 Is there an automatic fire protection system installed ABOVE the suspended ceiling in the computer ROOM?
YES -> jump 1 , NO -> jump 5

15.10 For the automatic fire protection system ABOVE the suspended ceiling in the computer ROOM, is the extinguishing agent a substance other than water?
YES -> jump 1 , NO -> jump 2

15.11 What is the extinguishing agent for the automatic fire protection system ABOVE the suspended ceiling in the computer ROOM: a) Halon, b) CO2, c) foam, d) other.
YES -> jump 1 , NO -> jump 1

15.12 Is there an adequate and nearby supply of the extinguishing agent for the automatic fire protection system ABOVE the suspended ceiling in the computer ROOM?
YES -> jump 1 , NO -> jump 1

15.13 Are sensors installed to detect water accumulation on the UPPER surface of the suspended ceiling in the computer ROOM?
YES -> jump 1 , NO -> jump 1

15.14 Is the area between the suspended ceiling and the structural ceiling in the computer ROOM kept free of dust and dirt?
YES -> jump 1 , NO -> jump 1

Category 16 : DATA CENTER MANAGEMENT

16. 1 Are checks of on-line security parameters made against a master copy at a frequency determined by data-center management?
YES -> jump 1 , NO -> jump 1

16. 2 Are there procedures for approving new or modified programming in any coding that affects the work of more than one person (e.g.,system or multi-user codes)?
YES -> jump 1 , NO -> jump 1

16. 3 Are random spot-checks run to compare on-line copies of essential software with master copies or source listings to detect unauthorized modification?
YES -> jump 1 , NO -> jump 1

16. 4 Are on-line copies of software checked periodically against their documentation to be sure that they are performing as anticipated?
YES -> jump 1 , NO -> jump 1

16. 5 Are standard test programs run frequently to check the validity of on-line software?
YES -> jump 1 , NO -> jump 1

16. 6 Are integrity and performance tests (like memory diagnostics) run after hardware maintenance and/or modification?
YES -> jump 1 , NO -> jump 1

16. 7 Are integrity and performance tests run after software maintenance and/or modification?
YES -> jump 1 , NO -> jump 1

16. 8 Are vendor-supplied software updates authenticated after they are received?
YES -> jump 1 , NO -> jump 3

16. 9 Is it required for vendor-supplied software updates to be identified as to the updater(s) in order to fix responsibility?
YES -> jump 1 , NO -> jump 1

16.10 Is it required that vendors supplying software updates either use a verified transmission channel or send updates in a verifiably-sealed package?
YES -> jump 1 , NO -> jump 1

16.11 Are all vendor-supplied software updates reviewed carefully before they are put on-line?
YES -> jump 1 , NO -> jump 1

16.12 Is it required that all vendor-supplied software updates must include source code for validation?
YES -> jump 1 , NO -> jump 1

16.13 Are vendor-supplied software updates validated by running them with known standard programs to assure that they function as expected?
YES -> jump 1 , NO -> jump 1

16.14 Are records of software modifications kept?
YES -> jump 1 , NO -> jump 3

16.15 Are records of software modifications kept in a safe location?
YES -> jump 1 , NO -> jump 1

16.16 Are there safeguards in place to assure that software modification records have been updated?
YES -> jump 1 , NO -> jump 1

16.17 Must there be more than one person involved to make any modifications to system or multi-user software?
YES -> jump 1 , NO -> jump 1

16.18 Does data-center management review authorization lists and system-usage logs to detect inactivity in user accounts?
YES -> jump 1 , NO -> jump 4

16.19 Is there a policy to repeal a user's authorizations if the user's account has been inactive for some time period determined by data-center management?
YES -> jump 1 , NO -> jump 2

16.20 If a user has not actually used the system in some specified time period, how long after this time period is it before the user's authorizations are repealed?
YES -> jump 1 , NO -> jump 1

16.21 Is the repeal of a user's authorization privileges called to the attention of all the appropriate personnel?
YES -> jump 1 , NO -> jump 1

16.22 Does data-center management employ user profiles to gain insight into program and data access patterns within the computer environment?
YES -> jump 1 , NO -> jump 4

16.23 Do the user profiles employed by data-center management yield insights into user accesses to specific programs?
YES -> jump 1 , NO -> jump 1

16.24 Do the user profiles employed by data-center management yield insights into USER accesses to specific data files?
YES -> jump 1 , NO -> jump 1

16.25 Do the user profiles employed by data-center management yield insights into PROGRAM accesses to specific data files?
YES -> jump 1 , NO -> jump 1

16.26 Are there controls for distributing reports and output containing sensitive, proprietary, or classified information?
YES -> jump 1 , NO -> jump 1

16.27 Are operating procedures for system operation documented?
YES -> jump 1 , NO -> jump 5

16.28 Are operating procedures documented for system startup?
YES -> jump 1 , NO -> jump 1

16.29 Are operating procedures documented for system shutdown?
YES -> jump 1 , NO -> jump 1

16.30 Are operating procedures for system restart or reboot documented?
YES -> jump 1 , NO -> jump 1

16.31 Are operating procedures documented for user access authorization?
YES -> jump 1 , NO -> jump 1

16.32 Are backups of documented procedures for system operation kept off-site?
YES -> jump 1 , NO -> jump 1

16.33 Does data-center management require that system backups are made frequently to ensure rapid recovery if a machine failure should occur?
YES -> jump 1 , NO -> jump 1

16.34 Is access to system diagnostics and memory dumps after machine failures limited to authorized persons?
YES -> jump 1 , NO -> jump 1

16.35 Does data-center management require that a record of all COMPUTER operations is kept, checked, and available for audit (if partially true, answer affirmatively)?
YES -> jump 1 , NO -> jump 6

16.36 Is a record of all COMPUTER operations kept?
YES -> jump 1 , NO -> jump 5

16.37 Does data-center management check the record of all COMPUTER operations?
YES -> jump 1 , NO -> jump 1

16.38 Is the record of all COMPUTER operations available for audit?
YES -> jump 1 , NO -> jump 1

16.39 Is the record of COMPUTER operations treated with the same level of security as the computer system?
YES -> jump 1 , NO -> jump 1

16.40 Is a backup of the COMPUTER-operations record kept off-site?
YES -> jump 1 , NO -> jump 1

16.41 Does data-center management require that a record of all operating-CONSOLE activity is kept, checked, and available for audit (if partially true, answer affirmatively)?
YES -> jump 1 , NO -> jump 6

16.42 Is a record of all operating-CONSOLE activity kept?
YES -> jump 1 , NO -> jump 5

16.43 Does data-center management check the record of all operating-CONSOLE activity?
YES -> jump 1 , NO -> jump 1

16.44 Is the record of operating-CONSOLE activity available for audit?
YES -> jump 1 , NO -> jump 1

16.45 Is the record of operating-CONSOLE activity treated with the same level of security as the computer system?
YES -> jump 1 , NO -> jump 1

16.46 Is a backup of the operating-CONSOLE activity record kept off-site?
YES -> jump 1 , NO -> jump 1

16.47 Are checks made to verify proper operation of on-line audit procedures?
YES -> jump 1 , NO -> jump 1

16.48 Is a record kept to provide accountability of system usage and user functions?
YES -> jump 1 , NO -> jump 7

16.49 Is there a record of program or task activity?
YES -> jump 1 , NO -> jump 1

16.50 Is there a record of cumulative job or session activity?
YES -> jump 1 , NO -> jump 1

16.51 Is there a record of cumulative accounting period activity?
YES -> jump 1 , NO -> jump 1

16.52 Are users informed regularly of account activity so that they could detect unauthorized use?
YES -> jump 1 , NO -> jump 1

16.53 Is the record of system usage and user functions treated with the same level of security as the computer system?
YES -> jump 1 , NO -> jump 1

16.54 Are backups of the records of system usage and user functions kept off-site?
YES -> jump 1 , NO -> jump 1

16.55 Has data-center management established a quality-assurance policy to assure that hardware and coding meet specifications and perform exactly as designed?
YES -> jump 1 , NO -> jump 6

16.56 Are there designated individuals who are responsible for quality assurance at the data center (i.e., is there an internal Q/A staff)?
YES -> jump 1 , NO -> jump 5

16.57 Are individuals who are responsible for internal quality assurance involved during the conceptual system design phase for hardware and/or software?
YES -> jump 1 , NO -> jump 1

16.58 Does the internal Q/A staff have sufficient knowledge about programming and hardware operation to assure that coding meets quality assurance design requirements?
YES -> jump 1 , NO -> jump 1

16.59 Are Q/A duties adequately separated and monitored to prevent coding manipulation?
YES -> jump 1 , NO -> jump 1

16.60 Is the internal Q/A staff informed of changes to programs or documentation of applications?
YES -> jump 1 , NO -> jump 1

16.61 Is smoking permitted in paper and supplies STORAGE AREA?
YES -> jump 1 , NO -> jump 1

16.62 Are beverages or food permitted in the STORAGE AREA for paper and supplies?
YES -> jump 1 , NO -> jump 1

Category 17 : DATA TRACEABILITY

17. 1 Are there verification controls for input data?
YES -> jump 1 , NO -> jump 5

17. 2 Is input data verified for sequence?
YES -> jump 1 , NO -> jump 1

17. 3 Is input data verified for completeness?
YES -> jump 1 , NO -> jump 1

17. 4 Is input data verified for range or reasonableness?
YES -> jump 1 , NO -> jump 1

17. 5 Is input data verified for consistency?
YES -> jump 1 , NO -> jump 1

17. 6 Do applications programs involve the use or storage of on-line data?
YES -> jump 1 , NO -> jump 2

17. 7 Are input source documents or magnetic media retained after the information is stored on-line?
YES -> jump 1 , NO -> jump 3

17. 8 Are multiple copies of source documents or magnetic media maintained in general?
YES -> jump 1 , NO -> jump 2

17. 9 Where are multiple copies of source documents or magnetic media kept?
YES -> jump 1 , NO -> jump 1

17.10 Are all forms of sensitive information (programs, data, output, reports in both human-readable and machine-readable versions) treated with the same level of control?
YES -> jump 1 , NO -> jump 1

17.11 Are audit trails of updates or modifications to applications software and data kept in general?
YES -> jump 1 , NO -> jump 3

17.12 Are on-line audit trails maintained on a disk volume separate from the main data file?
YES -> jump 1 , NO -> jump 1

17.13 Are on-line audit trails archived frequently?
YES -> jump 1 , NO -> jump 1

Category 18 : EMERGENCY & CONTINGENCY PLANNING

18. 1 Has a site been selected for local or SHORT-term contingency backup?
YES -> jump 1 , NO -> jump 9

18. 2 Is the local or SHORT-term contingency backup site located where it will not share interruptions with the home site and yet it can be reached conveniently?
YES -> jump 1 , NO -> jump 2

18. 3 Have written agreements with other agencies, service bureaus, and vendors been obtained for backup computer service at the SHORT-term contingency backup site?
YES -> jump 1 , NO -> jump 1

18. 4 Is there backup for all computer hardware at the local or SHORT-term contingency backup site?
YES -> jump 1 , NO -> jump 6

18. 5 Has the backup system for hardware at the local or SHORT-term contingency backup site been tested to insure compatibility with the applications?
YES -> jump 1 , NO -> jump 1

18. 6 Has backup for support equipment been identified and acquired for the local SHORT-term contingency backup site?
YES -> jump 1 , NO -> jump 4

18. 7 Are there backups for furniture at the local or SHORT-term contingency backup site?
YES -> jump 1 , NO -> jump 1

18. 8 Are there backups for essential office machines (eg, typewriters, word-processing equipment, copying machines) at the local or SHORT-term contingency backup site?
YES -> jump 1 , NO -> jump 1

18. 9 Has a preventive maintenance schedule been established for support equipment at the local or SHORT-term contingency backup site?
YES -> jump 1 , NO -> jump 1

18.10 Is a LONG-term contingency backup site (alternate site) deemed mission critical?
YES -> jump 1 , NO -> jump 35

18.11 Has a LONG-term contingency backup site (alternate site) been selected?
YES -> jump 1 , NO -> jump 34

18.12 Is the LONG-term contingency backup site located far enough from the home site that it will not share the same catastrophes (such as earthquakes, volcanic eruptions, major storms, etc)?
YES -> jump 1 , NO -> jump 1

18.13 Have written agreements with other agencies, service bureaus, and vendors been obtained for backup computer service at the LONG-term contingency backup site?
YES -> jump 1 , NO -> jump 1

18.14 Are security requirements for the equipment backups at the alternate site as stringent as at home?
YES -> jump 1 , NO -> jump 1

18.15 Are the design and operation of the alternate-site safeguards against natural hazards damage (major hazards, water, fire, HVAC, and power damage) as comprehensive as at home?
YES -> jump 1 , NO -> jump 5

18.16 Are safeguards against WATER DAMAGE as stringent at the alternate site as at home?
YES -> jump 1 , NO -> jump 1

18.17 Are safeguards against FIRE DAMAGE as stringent at the alternate site as at home?
YES -> jump 1 , NO -> jump 1

18.18 Are safeguards against HVAC DAMAGE as stringent at the alternate site as at home?
YES -> jump 1 , NO -> jump 1

18.19 Are safeguards against POWER OUTAGE DAMAGE as stringent at the alternate site as at home?
YES -> jump 1 , NO -> jump 1

18.20 Are safeguards against MAJOR HAZARDS DAMAGE as stringent at the alternate site as at home?
YES -> jump 1 , NO -> jump 1

18.21 Is there backup for facility support hardware (generators, HVAC, etc) at the LONG-term contingency backup site?
YES -> jump 1 , NO -> jump 20

18.22 Are there backups for the computer and its main components at the LONG-term contingency backup site?
YES -> jump 1 , NO -> jump 1

18.23 Have maintenance procedures been established for the computer and its main components at the LONG-term contingency backup site?
YES -> jump 1 , NO -> jump 1

18.24 Has the computer and its peripheral equipment at the LONG-term contingency backup site been tested to insure compatibility with the applications?
YES -> jump 1 , NO -> jump 1

18.25 Has backup for other data-processing equipment been identified and acquired at the LONG-term contingency backup site?
YES -> jump 1 , NO -> jump 4

18.26 Are there backups for terminal equipment at the LONG-term contingency backup site?
YES -> jump 1 , NO -> jump 1

18.27 Are there backups for off-line equipment (eg, forms bursters, film processors) at the LONG-term contingency backup site?
YES -> jump 1 , NO -> jump 1

18.28 Are there backups for data communications equipment at the LONG-term contingency backup site?
YES -> jump 1 , NO -> jump 1

18.29 Have hardware maintenance procedures been established for other data-processing equipment at the LONG-term contingency backup site?
YES -> jump 1 , NO -> jump 4

18.30 Are there maintenance procedures for terminal equipment at the LONG-term contingency backup site?
YES -> jump 1 , NO -> jump 1

18.31 Are there maintenance procedures for off-line equipment at the LONG-term contingency backup site?
YES -> jump 1 , NO -> jump 1

18.32 Has a preventive maintenance schedule been established for data communications equipment at the LONG-term contingency backup site?
YES -> jump 1 , NO -> jump 1

18.33 Has backup for support equipment (furniture, office machines, etc) been identified and acquired for the LONG-term contingency backup site?
YES -> jump 1 , NO -> jump 4

18.34 Are there backups for furniture at the LONG-term contingency backup site?
YES -> jump 1 , NO -> jump 1

18.35 Are there backups for office machines at the LONG-term contingency backup site?
YES -> jump 1 , NO -> jump 1

18.36 Are there backups for voice-communications equipment at the LONG-term contingency backup site?
YES -> jump 1 , NO -> jump 1

18.37 Have maintenance procedures been established for support equipment at the LONG-term contingency backup site?
YES -> jump 1 , NO -> jump 4

18.38 Are there maintenance procedures for furniture at the LONG-term contingency backup site?
YES -> jump 1 , NO -> jump 1

18.39 Are there maintenance procedures for office machines at the LONG-term contingency backup site?
YES -> jump 1 , NO -> jump 1

18.40 Are there maintenance procedures for voice-communications equipment at the LONG-term contingency backup site?
YES -> jump 1 , NO -> jump 1

18.41 Are backup copies of programs, data, and associated documentation stored at an alternate site away from the facility?
YES -> jump 1 , NO -> jump 4

18.42 Is more than one generation of backup files kept at the off-site storage location?
YES -> jump 1 , NO -> jump 1

18.43 Is the location of the off-site place for storing backup files public or common knowledge?
YES -> jump 1 , NO -> jump 1

18.44 Are security arrangements for backup software and documents at the off-site location as stringent as at home?
YES -> jump 1 , NO -> jump 1

Category 19 : EMERGENCY SITUATIONS & PROCEDURES

19. 1 Has a "Data Center Emergency Response Plan" (DCERP) been prepared?
YES -> jump 1 , NO -> jump 10

19. 2 Does the DCERP include a procedure for reporting incidents and notifying all personnel necessary to deal with an emergency situation?
YES -> jump 1 , NO -> jump 1

19. 3 Does the DCERP describe emergency and backup voice and data communications requirements?
YES -> jump 1 , NO -> jump 1

19. 4 Does the DCERP establish a plan for data center evacuation?
YES -> jump 1 , NO -> jump 1

19. 5 Does the DCERP include a strategy for fire emergencies?
YES -> jump 1 , NO -> jump 1

19. 6 Does the DCERP include a strategy to deal with water/flood emergencies?
YES -> jump 1 , NO -> jump 1

19. 7 Does the DCERP include a strategy to deal with power failures?
YES -> jump 1 , NO -> jump 1

19. 8 Does the DCERP include a strategy to deal with HVAC failures?
YES -> jump 1 , NO -> jump 1

19. 9 Does the DCERP include a strategy to deal with structural instabil or damage, such as that caused by earthquakes?
YES -> jump 1 , NO -> jump 1

19.10 Does the DCERP include a strategy for emergencies caused by weathe or other natural phenomena?
YES -> jump 1 , NO -> jump 1

19.11 Are all emergency response procedures for the data center reviewec least annually with data-center personnel?
YES -> jump 1 , NO -> jump 1

19.12 Are data-center personnel periodically drilled on all emergency response procedures?
YES -> jump 1 , NO -> jump 1

19.13 Are data-center fire drills practiced periodically?
YES -> jump 1 , NO -> jump 1

19.14 Have individuals been assigned specific responsibilities in case c fire?
YES -> jump 1 , NO -> jump 1

19.15 Are drills for bomb threats, terrorist attacks, or catastrophic events practiced periodically (answer affirmatively if any of thes are practiced)?
YES -> jump 1 , NO -> jump 4

19.16 Are drills for bomb threats practiced periodically?
YES -> jump 1 , NO -> jump 1

19.17 Are drills for terrorist attacks practiced periodically?
YES -> jump 1 , NO -> jump 1

19.18 Are drills for catastrophic events practiced periodically?
YES -> jump 1 , NO -> jump 1

19.19 Are location identifiers and emergency phone numbers posted in the computer center for fire, flood, police, on-site security, and medical assistance?
YES -> jump 1 , NO -> jump 1

19.20 Among the data center's personnel, are there persons with training for providing emergency medical assistance, cardiopulmonary resuscitation (CPR), and/or first aid?
YES -> jump 1 , NO -> jump 1

19.21 Are there always at least some on-duty computer-operations personnel who are trained in first aid and CPR?
YES -> jump 1 , NO -> jump 1

19.22 Are first-aid supplies located close enough for quick response in a medical emergency?
YES -> jump 1 , NO -> jump 1

19.23 Is there a generalized, established procedure for coordinating the movement of information and personnel in an emergency situation?
YES -> jump 1 , NO -> jump 1

19.24 If a breach of security occurred, do employees know where trained assistance is available?
YES -> jump 1 , NO -> jump 1

19.25 Are personnel instructed about how to deal with a penetration in progress?
YES -> jump 1 , NO -> jump 1

19.26 Is there a policy governing how personnel should interact with outside organizations and outside personnel with respect to security breaches and other emergencies?
YES -> jump 1 , NO -> jump 4

19.27 Is there a policy governing how personnel should interact with representatives of the news media with respect to security breaches and other emergencies?
YES -> jump 1 , NO -> jump 1

19.28 Is there a policy governing how personnel should interact with ot outside organizations with respect to security breaches and other emergencies?
YES -> jump 1 , NO -> jump 1

19.29 Is there a policy governing how personnel should interact with outside personnel (such as the public) with respect to security breaches and other emergencies?
YES -> jump 1 , NO -> jump 1

19.30 Is the staff instructed to protect prioritized hardware, software and documents from damage and/or disclosure if a disaster, major emergency, or an attack upon the data center occurs?
YES -> jump 1 , NO -> jump 1

19.31 Are data-center emergency/security systems backed up with battery power so they can continue operating if a power failure occurs?
YES -> jump 1 , NO -> jump 1

19.32 Do building security personnel and guards respond quickly when required by the data center in emergency situations?
YES -> jump 1 , NO -> jump 1

19.33 Do supporting services personnel (power, structural, communicatio water, sanitation engineers) respond quickly when required by the data center in emergency situations?
YES -> jump 1 , NO -> jump 1

19.34 Are there procedures to permit computer ROOM entry to emergency personnel in case of fire, serious power outage, or other emergen or disaster?
YES -> jump 1 , NO -> jump 1

19.35 Are watchmen or security personnel instructed about what to do if emergency occurs during non-working hours?
YES -> jump 1 , NO -> jump 1

19.36 Are watchmen or security personnel notified when emergency servic personnel are permitted access to the data center during emergenc situations?
YES -> jump 1 , NO -> jump 1

19.37 Do security or operations personnel monitor emergency service personnel when they are servicing the computer room, area, buildi or equipment?
YES -> jump 1 , NO -> jump 1

19.38 Are there fire doors to compartmentalize the BUILDING?
YES -> jump 1 , NO -> jump 2

19.39 Are the BUILDING's fire doors either closed automatically or secured manually when a fire is detected?
YES -> jump 1 , NO -> jump 1

19.40 Are there fire doors to compartmentalize the computer AREA in case of fire?
YES -> jump 1 , NO -> jump 2

19.41 Are AREA fire doors either closed automatically or secured manually in the event of a fire being detected?
YES -> jump 1 , NO -> jump 1

19.42 Are there fire doors to compartmentalize the computer ROOM in the event of a fire being detected?
YES -> jump 1 , NO -> jump 2

19.43 Are computer ROOM fire doors either closed automatically or secured manually in the event of a fire being detected?
YES -> jump 1 , NO -> jump 1

19.44 Is a complete set of vendor-recommended spare parts available near enough to the data center to be able to effect emergency repairs within the time period determined by facility management?
YES -> jump 1 , NO -> jump 1

19.45 Is an automatic fire PROTECTION (or sprinkler) system installed to protect against fires in the computer ROOM open space?
YES -> jump 1 , NO -> jump 7

19.46 What is the temperature rating of the automatic sprinkler head in the computer-ROOM ceiling (___ F.)?
YES -> jump 1 , NO -> jump 1

19.47 Is there an extinguishing agent other than water used in occupied areas by the automatic system?
YES -> jump 1 , NO -> jump 4

19.48 Is there a continuous supply or a nearby backup supply of the extinguishing agent for the automatic system in occupied areas?
YES -> jump 1 , NO -> jump 1

19.49 Is breathing apparatus available in well-known or clearly-marked locations in occupied areas to protect people from noxious or dangerous gaseous extinguishing agents?
YES -> jump 1 , NO -> jump 1

19.50 Are personnel made aware of the dangers of gaseous extinguishing agents in occupied areas and trained to work in pairs during emergency situations?
YES -> jump 1 , NO -> jump 1

19.51 Can the automatic fire PROTECTION system in occupied areas be controlled manually?
YES -> jump 1 , NO -> jump 1

19.52 Is an automatic fire PROTECTION system installed to protect against fires in COMPUTER ROOM equipment cabinets?
YES -> jump 1 , NO -> jump 3

19.53 Can the automatic fire PROTECTION system inside the equipment cabinets be activated manually?
YES -> jump 1 , NO -> jump 1

19.54 Is there a nearby backup supply of the extinguishing agent for the automatic fire PROTECTION system installed inside equipment cabinets
YES -> jump 1 , NO -> jump 1

19.55 Have staff and fire protection personnel reviewed and documented the location and operation of all automatic sprinkler shutoff valves?
YES -> jump 1 , NO -> jump 1

19.56 Are there portable fire extinguishers installed within the computer ROOM?
YES -> jump 1 , NO -> jump 5

19.57 Is there emergency lighting in the computer ROOM to illuminate fire extinguishers even if there is a power outage?
YES -> jump 1 , NO -> jump 1

19.58 Are fire extinguishers readily available throughout the entire computer ROOM with location and/or location markers visible to all computer room personnel?
YES -> jump 1 , NO -> jump 1

19.59 How many fire extinguishers are there in the computer ROOM?
YES -> jump 1 , NO -> jump 1

19.60 Are portable fire extinguishers in the computer ROOM tested periodically so that they have up-to-date certification?
YES -> jump 1 , NO -> jump 1

19.61 Have all personnel been instructed about how to use portable fire extinguishers?
YES -> jump 1 , NO -> jump 1

Category 20 : ENCRYPTION

20. 1 Is DATA-FILE encryption used at the data center?
YES -> jump 1 , NO -> jump 1

20. 2 Is APPLICATION-PROGRAM encryption used at the data center?
YES -> jump 1 , NO -> jump 1

20. 3 Is OUTPUT-FILE encryption used at the data center?
YES -> jump 1 , NO -> jump 1

Category 21 : FILES, STORAGE MEDIA, & DRIVES

21. 1 Are storage media other than those required for computer operations kept inside the computer ROOM instead of in a separate storage media LIBRARY?
YES -> jump 1 , NO -> jump 1

21. 2 Are there backups in a different location for any storage media kept in the computer ROOM (including those required for computer operations)?
YES -> jump 1 , NO -> jump 1

21. 3 Is the integrity of the file backup system tested at a frequency determined by data-center management?
YES -> jump 1 , NO -> jump 1

21. 4 Are special storage vaults used for essential storage media and files?
YES -> jump 1 , NO -> jump 1

21. 5 Are all storage media marked with classification (where appropriate), identity, contents, version, location, date, owner, and authorized users?
YES -> jump 1 , NO -> jump 1

21. 6 Are removable storage media (tapes, disks, diskettes) identified by codes rather than by verbal descriptors (e.g., "XYZ" rather than "PAYROLL")?
YES -> jump 1 , NO -> jump 1

21. 7 Are faulty storage media withdrawn from use?
YES -> jump 1 , NO -> jump 2

21. 8 Are all requests to use a storage medium screened for validity?
YES -> jump 1 , NO -> jump 1

21. 9 Are all invalid requests to use storage media recorded?
YES -> jump 1 , NO -> jump 1

21.10 Is a mechanism available to prevent someone from reading released storage media?
YES -> jump 1 , NO -> jump 2

21.11 What is the mechanism for preventing someone from reading released storage media?
YES -> jump 1 , NO -> jump 1

21.12 Does the hardware for storage media have error detection features?
YES -> jump 1 , NO -> jump 1

21.13 Does the hardware for handling storage media have reasonably complet error recovery features?
YES -> jump 1 , NO -> jump 1

21.14 Are methods provided for correcting an error made by peripheral devices and storage media?
YES -> jump 1 , NO -> jump 1

21.15 Do you know the error characteristics of the data center's disk drives, tape transports, and storage media?
YES -> jump 1 , NO -> jump 2

21.16 Does data-center management periodically review error characteristic to detect abnormal operation?
YES -> jump 1 , NO -> jump 1

21.17 Will errors by disk drives, tape transports, or storage media be detected and logged?
YES -> jump 1 , NO -> jump 1

21.18 Is preventive maintenance for storage devices performed periodically?
YES -> jump 1 , NO -> jump 4

21.19 Indicate how frequently preventive maintenance of storage devices is performed: a) daily, b) weekly, c) monthly, d) quarterly, e) yearly, f) other (specify).
YES -> jump 1 , NO -> jump 1

21.20 Are all disk packs and drives cleaned on a regularly-scheduled basis?
YES -> jump 1 , NO -> jump 1

21.21 Are all tapes and tape drives cleaned regularly? (If tapes are not used, answer Y)
YES -> jump 1 , NO -> jump 1

Category 22 : GENERAL LOCALE

22. 1 Do the facility and the data center have a history of exposure to any major natural disasters (such as earthquakes, volcanic eruptions, tornadoes or hurricanes, forest or brush fires, and so forth)?
YES -> jump 1 , NO -> jump 1

22. 2 Are the facility and the data center located near an active earthquake fault?
YES -> jump 1 , NO -> jump 1

22. 3 Are the facility and the data center located near an active volcano?
YES -> jump 1 , NO -> jump 1

22. 4 Are the facility and the data center located near a source of flooding, such as near a river or a large body of water?
YES -> jump 1 , NO -> jump 1

22. 5 Are the facility and the data center located below a nearby dam?
YES -> jump 1 , NO -> jump 1

22. 6 Are the facility and the data center located in or near a forest, in heavy brush, or in a grassland area?
YES -> jump 1 , NO -> jump 1

22. 7 Are the facility and the data center located in a landslide or mudslide area?
YES -> jump 1 , NO -> jump 1

22. 8 Are the facility and the data center located in an area that has severe electrical storms (thunderstorms) or torrential rains?
YES -> jump 1 , NO -> jump 1

22. 9 Are the facility and the data center located in an area that is exposed to severe windstorms (such as a tornado or a hurricane)?
YES -> jump 1 , NO -> jump 1

22.10 Are the facility and the data center near a place where hazardous processes or materials are in use (such as a chemical plant, refinery, etc.)?
YES -> jump 1 , NO -> jump 1

22.11 Are the facility and data center located along a route used for transporting hazardous or explosive materials?
YES -> jump 1 , NO -> jump 1

22.12 Are the facility and the data center near an airfield, an airport, or an Air Force base?
YES -> jump 1 , NO -> jump 1

22.13 Do aircraft regularly fly over the data center (aircraft definition includes gliders; "fly over" includes normal flight paths)?
YES -> jump 1 , NO -> jump 1

22.14 Are the facility and the data center near any other potential source of hazard?
YES -> jump 1 , NO -> jump 2

22.15 Specify other potential sources of hazard near the facility in general and the data center in particular.
YES -> jump 1 , NO -> jump 1

22.16 Is this data center considered to be a showcase data center (frequently having tours or visitors from the general public)?
YES -> jump 1 , NO -> jump 1

22.17 Are the facility and the data center in a low-crime-rate area?
YES -> jump 1 , NO -> jump 1

22.18 Is the facility or the data center a potential target because of its mission or the nature of the work done there?
YES -> jump 1 , NO -> jump 1

22.19 Are there other occupants or activities in the BUILDING housing the data center that might be a potential threat or hazard to the data center, personnel, facility, or the organization's environment?
YES -> jump 1 , NO -> jump 2

22.20 What other occupants or activities in the BUILDING may be a potential hazard? a) offices, b) laboratory(s), c) machine shops, d) warehouses, e) chemical storerooms, f) other (specify).
YES -> jump 1 , NO -> jump 1

Category 23 : HEATING, VENTILATION, & AIR CONDITIONING

23. 1 Is there an air-conditioning system in use for the computer ROOM?
YES -> jump 1 , NO -> jump 10

23. 2 Is the cooling capacity of the air-conditioning equipment sufficient for the requirements of the computer ROOM?
YES -> jump 1 , NO -> jump 1

23. 3 Is the air-conditioning system used exclusively for the computer ROOM?
YES -> jump 1 , NO -> jump 1

23. 4 Is there an independent backup for the computer ROOM air-conditioning system?
YES -> jump 1 , NO -> jump 1

23. 5 Are air-conditioning filters fire resistant?
YES -> jump 1 , NO -> jump 1

23. 6 Is the air-conditioning equipment covered by a preventive maintenance program?
YES -> jump 1 , NO -> jump 1

23. 7 Is the compressor and related air-conditioning equipment serviced on a regular schedule?
YES -> jump 1 , NO -> jump 1

23. 8 Does the air-conditioning system include humidity control?
YES -> jump 1 , NO -> jump 1

23. 9 Is external air-conditioning equipment (eg, cooling towers, chillers, compressors) appropriately protected from both natural and human threats?
YES -> jump 1 , NO -> jump 1

23.10 Can the computer ROOM air-conditioning system be shut off manually from within the computer room?
YES -> jump 1 , NO -> jump 1

23.11 Are air intakes protected from accidental and/or deliberate air contamination?
YES -> jump 1 , NO -> jump 1

23.12 Is there an automatic monitoring system (with alarms) for the heating/ventilating/air-conditioning (HVAC) system used for the computer ROOM?
YES -> jump 1 , NO -> jump 6

23.13 Is air-conditioning failure or shutdown monitored with an alarm?
YES -> jump 1 , NO -> jump 1

23.14 Is airflow restriction or failure monitored with an alarm?
YES -> jump 1 , NO -> jump 1

23.15 Are temperature-rise limits/rate monitored with an alarm?
YES -> jump 1 , NO -> jump 1

23.16 Is humidity monitored with an alarm?
YES -> jump 1 , NO -> jump 1

23.17 Is immediate action taken by operations personnel when the automatic HVAC monitoring system alarm sounds in the computer ROOM?
YES -> jump 1 , NO -> jump 1

23.18 Do alarms from the automatic monitoring system for the heating/ventilating/air-conditioning (HVAC) system used for the computer ROOM transmit to locations outside the computer ROOM?
YES -> jump 1 , NO -> jump 6

23.19 Does an alarm for air-conditioning failure or shutdown transmit to a location outside the computer ROOM?
YES -> jump 1 , NO -> jump 1

23.20 Does an alarm for airflow restriction or failure transmit to a location outside the computer ROOM?
YES -> jump 1 , NO -> jump 1

23.21 Does an alarm for temperature-rise limits and/or rate transmit to a location outside the computer ROOM?
YES -> jump 1 , NO -> jump 1

23.22 Does an alarm for out-of-range humidity transmit to somewhere outside the computer ROOM?
YES -> jump 1 , NO -> jump 1

23.23 Is immediate action taken by appropriate personnel when the automatic HVAC monitoring system alarm transmission is received?
YES -> jump 1 , NO -> jump 1

23.24 Is there an automatic HVAC monitoring system with a computer-shutdown capability for the computer ROOM?
YES -> jump 1 , NO -> jump 6

23.25 Will air-conditioning failure or shutdown automatically trigger a computer shutdown?
YES -> jump 1 , NO -> jump 1

23.26 Will airflow restriction or failure automatically trigger a computer shutdown?
YES -> jump 1 , NO -> jump 1

23.27 Will exceeding temperature-rise limits and/or rate automatically trigger a computer shutdown?
YES -> jump 1 , NO -> jump 1

23.28 Will a computer shutdown result from exceeding humidity range limits?
YES -> jump 1 , NO -> jump 1

23.29 Is manual intervention required to restore power to the computer following an automatic shutdown caused by such HVAC monitoring functions?
YES -> jump 1 , NO -> jump 1

Category 24 : HOUSEKEEPING & MAINTENANCE

24. 1 Is an industrial wet/dry vacuum cleaner available for use in the BUILDING?
YES -> jump 1 , NO -> jump 1

24. 2 Is the computer ROOM cleaned on a regular schedule?
YES -> jump 1 , NO -> jump 1

24. 3 Is the computer ROOM kept free of dust and clutter?
YES -> jump 1 , NO -> jump 1

24. 4 Are equipment covers and work surfaces cleaned frequently?
YES -> jump 1 , NO -> jump 1

24. 5 Is all computer-ROOM equipment kept free of dust and dirt inside and out?
YES -> jump 1 , NO -> jump 1

24. 6 Are computer-ROOM floors cleaned regularly with a non-residual cleaning agent?
YES -> jump 1 , NO -> jump 1

24. 7 Is all computer equipment covered by a preventive maintenance program?
YES -> jump 1 , NO -> jump 1

24. 8 Is preventive maintenance of critical systems equipment, such as the CPU, performed periodically?
YES -> jump 1 , NO -> jump 2

24. 9 Indicate how frequently preventive maintenance of critical equipment is performed: a) daily, b) weekly, c) monthly, d) quarterly, e) yearly, f) other (specify).
YES -> jump 1 , NO -> jump 1

24.10 Is preventive maintenance of disk drives performed periodically?
YES -> jump 1 , NO -> jump 4

24.11 Indicate how frequently preventive maintenance of disk drives is performed: a) daily, b) weekly, c) monthly, d) quarterly, e) yearly, f) other (specify).
YES -> jump 1 , NO -> jump 1

24.12 Are all heads on disk drives cleaned on a regularly-scheduled basis? (Cleaning not required with sealed drives.)
YES -> jump 1 , NO -> jump 1

24.13 Is the alignment of disk-drive heads checked regularly? (Not required with sealed drives.)
YES -> jump 1 , NO -> jump 1

24.14 Is preventive maintenance of peripheral computer system equipment performed periodically?
YES -> jump 1 , NO -> jump 2

24.15 Indicate how frequently preventive maintenance of peripheral equipment is performed: a) daily, b) weekly, c) monthly, d) quarterly, e) yearly, f) other (specify).
YES -> jump 1 , NO -> jump 1

24.16 Is a complete set of vendor-recommended spare parts available near enough to the computer center to be able to effect routine maintenance and repairs in a timely manner?
YES -> jump 1 , NO -> jump 1

Category 25 : INVENTORY PROCEDURES & POLICY

25. 1 Is a facility-wide inventory of office equipment and supplies, hardware, software, and documents conducted at least yearly for the facility and the data center?
YES -> jump 1 , NO -> jump 11

25. 2 Are there inventory lists of equipment, machine-readable files, and documents?
YES -> jump 1 , NO -> jump 10

25. 3 Is the facility-wide inventory list updated periodically as determined by facility management?
YES -> jump 1 , NO -> jump 1

25. 4 Is there a current inventory list of the major equipment within the data center?
YES -> jump 1 , NO -> jump 1

25. 5 Is there a current inventory list of system, application, and data files for which the data center has responsibility?
YES -> jump 1 , NO -> jump 4

25. 6 Does the current inventory list include a systems software inventory?
YES -> jump 1 , NO -> jump 1

25. 7 Does the current inventory list include an applications inventory?
YES -> jump 1 , NO -> jump 1

25. 8 Does the current inventory list include a list of essential or critical data files?
YES -> jump 1 , NO -> jump 1

25. 9 Does the current inventory list contain an inventory of documentation and reports?
YES -> jump 1 , NO -> jump 1

25.10 Are backups of inventory lists (of equipment, files, and documents) kept off-site?
YES -> jump 1 , NO -> jump 1

25.11 Is there an established procedure for resolving discrepancies in the facility and/or data center inventories of equipment, files, and documents?
YES -> jump 1 , NO -> jump 1

Category 26 : MANAGEMENT ISSUES & POLICY

26. 1 Does your organization require commercial insurance (is it otherwise unable financially to survive catastrophic damage to property, equipment, information, or personnel)?
YES -> jump 1 , NO -> jump 7

26. 2 Is the ORGANIZATION and all its related equipment insured?
YES -> jump 1 , NO -> jump 6

26. 3 Is the BUILDING and all related equipment insured?
YES -> jump 1 , NO -> jump 1

26. 4 Is all computer hardware, storage media, storage devices, and other peripheral and support equipment, insured?
YES -> jump 1 , NO -> jump 1

26. 5 Is all the machine-readable information, including operating systems, applications programs, and data and output files in machine-readable form, insured?
YES -> jump 1 , NO -> jump 1

26. 6 Is all human-readable information, including operations manuals, applications programs manuals and listings, data and output copy, reports, memos, and letters, insured?
YES -> jump 1 , NO -> jump 1

26. 7 Is there liability insurance for personal injury?
YES -> jump 1 , NO -> jump 1

26. 8 Does the facility/site/base have an enforced limited-access policy?
YES -> jump 1 , NO -> jump 1

26. 9 Does a lobby directory, site map, facility description, or other publicly-available or posted document clearly pinpoint the location of the data center?
YES -> jump 1 , NO -> jump 1

26.10 Is there documentation pinpointing the data-center location that has widespread public dissemination?
YES -> jump 1 , NO -> jump 1

26.11 Is there documentation clearly pinpointing data-center location that is well-known and distributed widely throughout the facility/site/base?
YES -> jump 1 , NO -> jump 1

26.12 Are background checks made on all new employes?
YES -> jump 1 , NO -> jump 2

26.13 Are periodic follow-up background checks made on employes after employment?
YES -> jump 1 , NO -> jump 1

26.14 Are all employes given regular performance appraisals and the opportunity to discuss with management their thoughts about their jobs, their co-workers and their supervisors?
YES -> jump 1 , NO -> jump 1

26.15 Is it policy to train managers and supervisors to recognize and report changes in personal behavior and habits to senior management or a facility department/group delegated to deal with such problems?
YES -> jump 1 , NO -> jump 5

26.16 Are managers and supervisors trained to recognize signs of job performance being affected by drug or alcohol abuse?
YES -> jump 1 , NO -> jump 1

26.17 Are supervisors trained/instructed to bring to management's attention personnel exhibiting signs of poor job performance attributable to suspected drug or alcohol abuse?
YES -> jump 1 , NO -> jump 1

26.18 Are managers aware that sudden or unusually large accumulations of vacation and/or sick leave are potential indicators of privilege abuse?
YES -> jump 1 , NO -> jump 1

26.19 Are supervisors trained/instructed to bring to management's attention personnel who have accumulated unusually large amounts of leave?
YES -> jump 1 , NO -> jump 1

26.20 Are supervisors and management close enough to personnel to detect changes in working, living, and personal habits?
YES -> jump 1 , NO -> jump 1

26.21 Is line management aware of the potential effect of low morale or disgruntled employes?
YES -> jump 1 , NO -> jump 1

26.22 Has facility/site/base management established a policy for personal conduct of employes?
YES -> jump 1 , NO -> jump 2

26.23 Does management keep personnel informed about rules of personal conduct?
YES -> jump 1 , NO -> jump 1

26.24 Does policy permit the immediate removal or relocation for cause of an employe from areas in which the employe may potentially do harm?
YES -> jump 1 , NO -> jump 1

26.25 Has senior facility/site/base management shown an awareness of the special security needs of the data center?
YES -> jump 1 , NO -> jump 1

26.26 Is data-center management involved in establishing facility/site/base security procedures and/or data-center security procedures?
YES -> jump 1 , NO -> jump 1

26.27 Are PERSONNEL educated about security practices and encouraged to be alert at all times?
YES -> jump 1 , NO -> jump 5

26.28 Is the DATA CENTER STAFF educated about security practices and encouraged to be alert at all times?
YES -> jump 1 , NO -> jump 1

26.29 Are DATA CENTER USERS educated about security practices and encouraged to be alert at all times?
YES -> jump 1 , NO -> jump 1

26.30 Are CUSTODIAL PERSONNEL educated about security practices and encouraged to be alert at all times?
YES -> jump 1 , NO -> jump 1

26.31 Are MAINTENANCE PERSONNEL educated about security practices and encouraged to be alert at all times?
YES -> jump 1 , NO -> jump 1

26.32 Are personnel given continuing or periodic refresher education about security practices?
YES -> jump 1 , NO -> jump 1

26.33 Is senior management aware of the costs (both tangible and intangible) associated with lost or compromised information (software, documents)?
YES -> jump 1 , NO -> jump 1

26.34 Are all forms of sensitive information (programs, data, output, reports in both human-readable and machine-readable versions) treated with the same level of control?
YES -> jump 1 , NO -> jump 1

26.35 Do independent auditors check facilities, operations, and applications periodically?
YES -> jump 1 , NO -> jump 1

26.36 Are key data center functions defined in a document?
YES -> jump 1 , NO -> jump 5

26.37 Is the system management function defined in a document?
YES -> jump 1 , NO -> jump 1

26.38 Is the system operations function defined in a document?
YES -> jump 1 , NO -> jump 1

26.39 Is the system software maintenance function defined in a document?
YES -> jump 1 , NO -> jump 1

26.40 Is the computer equipment maintenance function defined in a document?
YES -> jump 1 , NO -> jump 1

26.41 Have individuals been assigned to be responsible for key data-center functions?
YES -> jump 1 , NO -> jump 5

26.42 Has an individual been assigned to be responsible for the system management function?
YES -> jump 1 , NO -> jump 1

26.43 Have individuals been assigned to be responsible for the system operations function?
YES -> jump 1 , NO -> jump 1

26.44 Have individuals been assigned the system software maintenance function responsibility?
YES -> jump 1 , NO -> jump 1

26.45 Have individuals been assigned the computer equipment maintenance function responsibility?
YES -> jump 1 , NO -> jump 1

26.46 Is it policy that one person cannot perform a complete set of transactions for an operation or application (eg, separate personnel for systems programming and for computer operations)?
YES -> jump 1 , NO -> jump 1

26.47 Is there policy to assure that key or sensitive jobs are rotated periodically?
YES -> jump 1 , NO -> jump 1

26.48 Is it a policy that no essential function can be performed by only one person (i.e., a multiple-person rule for all essential functions)?
YES -> jump 1 , NO -> jump 1

26.49 Is there a policy or an effective authorization procedure used for removing computer equipment, parts, data, or documentation from the BUILDING?
YES -> jump 1 , NO -> jump 6

26.50 Is there a policy or an effective authorization procedure used for removing COMPUTER EQUIPMENT AND PARTS from the BUILDING?
YES -> jump 1 , NO -> jump 1

26.51 Is there policy or an effective authorization procedure used for removing STORAGE MEDIA AND MEMORY DEVICES from the BUILDING?
YES -> jump 1 , NO -> jump 1

26.52 Is there policy or an effective authorization procedure used for removing computer PRINTOUTS and DOCUMENTATION from the BUILDING?
YES -> jump 1 , NO -> jump 3

26.53 Is it policy for a knowledgeable person to inspect FAILED parts and equipment before they can be removed from the BUILDING?
YES -> jump 1 , NO -> jump 1

26.54 Is there a known way to avoid or defeat the authorization procedure for removing computer equipment, data, or documentation from the BUILDING?
YES -> jump 1 , NO -> jump 1

26.55 Is it policy that personnel using the data center are held responsible for a clean working environment?
YES -> jump 1 , NO -> jump 1

26.56 Are there standard operating procedures (SOPs) for advising data-center personnel of emergencies and hazardous weather conditions?
YES -> jump 1 , NO -> jump 1

26.57 Is a public-address system used at the facility/site/base for quickly notifying personnel of emergencies, hazardous weather conditions, and so forth?
YES -> jump 1 , NO -> jump 3

26.58 Does the public-address system announcer practice canned messages so that message quality is consistent and does not suffer from the potential panic of an emergency?
YES -> jump 1 , NO -> jump 1

26.59 Can the public-address system be clearly heard and understood by all personnel?
YES -> jump 1 , NO -> jump 1

26.60 Will appropriate computer ROOM personnel be notified of nearby disasters and/or threats that may affect computer operations?
YES -> jump 1 , NO -> jump 1

Category 27 : NEGOTIABLE FINANCIAL DOCUMENTS

27. 1 Are negotiable or financial documents processed at the computer facility?
YES -> jump 1 , NO -> jump 8

27. 2 When negotiable or financial documents are produced, are there controls governing their issue, return, and accountability (if partially controlled, answer yes)?
YES -> jump 1 , NO -> jump 4

27. 3 When negotiable or financial documents are produced, are there controls governing their issue?
YES -> jump 1 , NO -> jump 1

27. 4 When negotiable or financial documents are produced, are there controls governing their return?
YES -> jump 1 , NO -> jump 1

27. 5 When negotiable or financial documents are produced, are there controls governing their accountability?
YES -> jump 1 , NO -> jump 1

27. 6 Are all negotiable or financial document sets numbered?
YES -> jump 1 , NO -> jump 1

27. 7 Are all negotiable or financial documents signed by the appropriate authority AFTER being processed in the computer center rather than being pre-signed or pre-stamped?
YES -> jump 1 , NO -> jump 1

27. 8 Are all spoiled or unusable negotiable or financial documents destroyed to prevent their misuse?
YES -> jump 1 , NO -> jump 1

Category 28 : PASSWORDS

28. 1 Is a password required for a user to gain access to the computer system?
YES -> jump 1 , NO -> jump 47

28. 2 Is someone responsible for changing all initial (vendor-provided) passwords before allowing the general user population access to the computer system?
YES -> jump 1 , NO -> jump 1

28. 3 Is somebody responsible for generating and assigning the initial password for each user ID?
YES -> jump 1 , NO -> jump 3

28. 4 Are user IDs always validated when initial passwords are assigned?
YES -> jump 1 , NO -> jump 1

28. 5 Can the system security officer (SSO) enter the initial classification assignment to designate the highest security level that may be associated with a user's initial and successive passwords?
YES -> jump 1 , NO -> jump 1

28. 6 Must users send an acknowledgment to the system security officer upon receiving a password?
YES -> jump 1 , NO -> jump 1

28. 7 Is it policy that associated passwords are removed from the system when a user leaves the organization or a project?
YES -> jump 1 , NO -> jump 1

28. 8 Is somebody responsible for seeing that all passwords are changed at a frequency commensurate with the length of the password and the necessary security level?
YES -> jump 1 , NO -> jump 1

28. 9 Is it policy that passwords must not be exposed during their generation, distribution, receipt, and use?
YES -> jump 1 , NO -> jump 1

28.10 Are passwords required to be at least six characters long?
YES -> jump 1 , NO -> jump 1

28.11 Are all passwords created by a statistical (or random) generation algorithm?
YES -> jump 1 , NO -> jump 3

28.12 Is the minimum number of possible passwords (minimum possible password space) generated by the random password-generation algorithm at least 50 million?
YES -> jump 1 , NO -> jump 1

28.13 Does the password-generation algorithm assure that the passwords are not generated in a reproducible or predictable manner?
YES -> jump 1 , NO -> jump 1

28.14 Does more than one person know the mapping of specific user IDs and associated passwords?
YES -> jump 1 , NO -> jump 1

28.15 Is there a maximum lifetime for all passwords?
YES -> jump 1 , NO -> jump 4

28.16 Are user IDs "locked" (no further access permitted) upon password expiration?
YES -> jump 1 , NO -> jump 1

28.17 Is the maximum lifetime of a password sufficiently short, taking into consideration the information sensitivity and attractiveness, potential threats, and password length?
YES -> jump 1 , NO -> jump 1

28.18 Are passwords long enough, taking into account their maximum lifetime, to prevent their being easily broken?
YES -> jump 1 , NO -> jump 1

28.19 Are preventive measures taken to assure that system users cannot read the password database?
YES -> jump 1 , NO -> jump 1

28.20 Is there a documented or enforced password change procedure?
YES -> jump 1 , NO -> jump 3

28.21 Is the password change procedure documented?
YES -> jump 1 , NO -> jump 1

28.22 Is the password change procedure enforced?
YES -> jump 1 , NO -> jump 1

28.23 Are user IDs always validated as part of the password change procedure?
YES -> jump 1 , NO -> jump 2

28.24 Are user IDs revalidated periodically in a time frame determined by the sensitivity of the information being processed?
YES -> jump 1 , NO -> jump 1

28.25 Is the password change procedure always invoked when a user attempts to access the system with an expired password?
YES -> jump 1 , NO -> jump 1

28.26 Can a password change be invoked by a user's request at login time?
YES -> jump 1 , NO -> jump 2

28.27 Must a user always enter his/her present password to re-authenticate the user's ID when he/she is attempting to change his/her present password?
YES -> jump 1 , NO -> jump 1

28.28 Are system users required to report any password security violations, including those associated with unauthorized password generation, distribution, or use?
YES -> jump 1 , NO -> jump 1

28.29 Are system users required to report changes in their privileges status or in the status of their data in order to maintain the integrity of the password system?
YES -> jump 1 , NO -> jump 1

28.30 Are ALL passwords considered to require security commensurate with the security level of the information being processed?
YES -> jump 1 , NO -> jump 1

28.31 Is the computer-based master list of passwords encrypted?
YES -> jump 1 , NO -> jump 1

28.32 Is the means used to communicate passwords to users commensurate with the security level of the information being processed?
YES -> jump 1 , NO -> jump 1

28.33 Is the echoing display of ALL passwords suppressed automatically?
YES -> jump 1 , NO -> jump 1

28.34 Is some defensive action triggered by exceeding a specified maximum NUMBER of invalid password attempts?
YES -> jump 1 , NO -> jump 4

28.35 What is the maximum NUMBER of invalid password attempts permitted before action is triggered?
YES -> jump 1 , NO -> jump 1

28.36 Is the maximum NUMBER of invalid password attempts permitted before triggering a defensive action commensurate with the minimum password length and the maximum password lifetime?
YES -> jump 1 , NO -> jump 1

28.37 Are technical and site security personnel automatically involved in restoring privileges to a user if he has exceeded the maximum NUMBER of invalid password attempts?
YES -> jump 1 , NO -> jump 1

28.38 Is some defensive action triggered after exceeding some specified FREQUENCY of invalid password attempts?
YES -> jump 1 , NO -> jump 4

28.39 What is the specified FREQUENCY of invalid password attempts that will trigger defensive action?
YES -> jump 1 , NO -> jump 1

28.40 Is the maximum FREQUENCY of invalid password attempts commensurate with the password's minimum length and maximum lifetime?
YES -> jump 1 , NO -> jump 1

28.41 Are technical and site security automatically involved in restoring user privileges after defensive action has been triggered for exceeding the maximum FREQUENCY of invalid password attempts?
YES -> jump 1 , NO -> jump 1

28.42 Are ANY attempts at password usage written into the computer-based audit record?
YES -> jump 1 , NO -> jump 3

28.43 Are INVALID attempts at password usage written into the computer-based audit record?
YES -> jump 1 , NO -> jump 1

28.44 Are VALID attempts at password usage written into the computer-based audit record?
YES -> jump 1 , NO -> jump 1

28.45 Are passwords changed at least yearly?
YES -> jump 1 , NO -> jump 1

28.46 Is it facility management's policy to instruct users to protect their passwords?
YES -> jump 1 , NO -> jump 1

28.47 Do users face penalties for not protecting passwords?
YES -> jump 1 , NO -> jump 1

Category 29 : PERIMETER ZONE

29. 1 Is unauthorized vehicular activity both prohibited and prevented in the perimeter?
YES -> jump 1 , NO -> jump 1

29. 2 Does the facility's physical environment include a PERIMETER ZONE of grounds and/or property surrounding the facility?
YES -> jump 1 , NO -> jump 61

29. 3 Does security require all personnel, regardless of their rank, to sign in or be properly identifiable to enter the facility's property or PERIMETER ZONE?
YES -> jump 1 , NO -> jump 1

29. 4 Does the PERIMETER ZONE surrounding the facility's property have a fence or other barrier restricting entry?
YES -> jump 1 , NO -> jump 47

29. 5 Is the PERIMETER barrier either a reinforced concrete wall or a chain-link fence?
YES -> jump 1 , NO -> jump 1

29. 6 How many entrances to the PERIMETER ZONE are there?
YES -> jump 1 , NO -> jump 1

29. 7 When are PERIMETER entrances available for general use (exclude special-purpose entrances or those requiring special authority or having special controls)?
YES -> jump 1 , NO -> jump 1

29. 8 Are there redundant barriers (e.g., double fences) or additional deterrents (e.g., barbed wire, electrified wire, sensors) attached to the PERIMETER barrier?
YES -> jump 1 , NO -> jump 2

29. 9 What is the additional PERIMETER barrier or deterrent? a) barbed wire above, b) barbed wire and razor ribbon, c) broken glass atop masonry, d) electrified wire, e) double fence, f) other.
YES -> jump 1 , NO -> jump 1

29.10 Is the minimum height of the PERIMETER barrier at least 8 feet?
YES -> jump 1 , NO -> jump 1

29.11 Is the minimum distance from the PERIMETER barrier to the building housing the data center at least 50 feet?
YES -> jump 1 , NO -> jump 1

29.12 Is someone responsible for periodically verifying the structural integrity of the perimeter barrier?
YES -> jump 1 , NO -> jump 1

29.13 Is there a designated individual(s) responsible for authorizing PERIMETER ZONE entry?
YES -> jump 1 , NO -> jump 2

29.14 State who is responsible for authorizing PERIMETER ZONE entry.
YES -> jump 1 , NO -> jump 1

29.15 Are there effective procedures in place for authorizing PERIMETER ZONE entry?
YES -> jump 1 , NO -> jump 3

29.16 Is there an independent verification of the requests for PERIMETER entry authorization?
YES -> jump 1 , NO -> jump 1

29.17 Is positive identification required for a person to receive authorization for PERIMETER entry?
YES -> jump 1 , NO -> jump 1

29.18 Are entrances or gates to the PERIMETER ZONE controlled (several questions follow about HOW and WHEN if this question is answered Y)?
YES -> jump 1 , NO -> jump 23

29.19 Are all entrances to the PERIMETER ZONE controlled DURING normal working hours?
YES -> jump 1 , NO -> jump 1

29.20 Are all entrances to the PERIMETER ZONE controlled AFTER normal working hours?
YES -> jump 1 , NO -> jump 1

29.21 Are all entrances to the PERIMETER ZONE controlled DURING EMERGENCIES?
YES -> jump 1 , NO -> jump 1

29.22 Is entry to the PERIMETER ZONE controlled by a GUARD(s)?
YES -> jump 1 , NO -> jump 2

29.23 How does the guard permit entry to the PERIMETER ZONE? a) by verifying ID from a list, b) by visual recognition, c) check badge with no photo, d) check badge with photo, e) other.
YES -> jump 1 , NO -> jump 1

29.24 Is entry to the PERIMETER ZONE controlled by a KEY?
YES -> jump 1 , NO -> jump 3

29.25 How many persons have keys to the PERIMETER ZONE?
YES -> jump 1 , NO -> jump 1

29.26 Is it difficult to duplicate keys to the PERIMETER ZONE (ie, do keys carry engraved instructions prohibiting their duplication, are they made from non-standard blanks, etc.)?
YES -> jump 1 , NO -> jump 1

29.27 Is entry to the PERIMETER ZONE controlled by a CIPHER LOCK?
YES -> jump 1 , NO -> jump 3

29.28 How many persons have the combination to the cipher lock controlling entry to the PERIMETER ZONE?
YES -> jump 1 , NO -> jump 1

29.29 Is the combination to the PERIMETER ZONE's cipher lock changed periodically?
YES -> jump 1 , NO -> jump 1

29.30 Is entry to the PERIMETER ZONE controlled by MAGNETIC CARD/BADGE READERS?
YES -> jump 1 , NO -> jump 2

29.31 How many persons have magnetic cards/badges permitting entry to the PERIMETER ZONE?
YES -> jump 1 , NO -> jump 1

29.32 Are vehicles permitted within the PERIMETER ZONE?
YES -> jump 1 , NO -> jump 9

29.33 Are vehicles permitted TO PARK within the PERIMETER ZONE?
YES -> jump 1 , NO -> jump 4

29.34 Are employes and contractors permitted to park their personal vehicles within the PERIMETER ZONE?
YES -> jump 1 , NO -> jump 1

29.35 Are service personnel permitted to park within the PERIMETER ZONE?
YES -> jump 1 , NO -> jump 1

29.36 Are visitors who are not service personnel permitted to park within the PERIMETER ZONE?
YES -> jump 1 , NO -> jump 1

29.37 Are there procedures for inspecting ALL vehicles permitted within the PERIMETER ZONE?
YES -> jump 1 , NO -> jump 4

29.38 Are vehicles searched when entering the PERIMETER ZONE?
YES -> jump 1 , NO -> jump 1

29.39 Are vehicles searched when leaving the PERIMETER ZONE?
YES -> jump 1 , NO -> jump 1

29.40 Are all individual members of a group entering or leaving the PERIMETER ZONE in the same vehicle checked for authorization and identification?
YES -> jump 1 , NO -> jump 1

29.41 Are authorization lists and control mechanisms permitting entry to the PERIMETER ZONE updated when a person is no longer authorized for perimeter-zone entry?
YES -> jump 1 , NO -> jump 2

29.42 When a person is no longer authorized for entry to the PERIMETER ZONE, are a) authorization lists revised, b) locks and/or combinations changed, c) keys/cards/badges surrendered, d) other.
YES -> jump 1 , NO -> jump 1

29.43 Is access to the PERIMETER ZONE and to resources denied quickly enough to prevent damage to resources by a person who no longer is authorized for entry to the PERIMETER ZONE?
YES -> jump 1 , NO -> jump 1

29.44 Are any entries to or exits from the PERIMETER ZONE recorded at any time?
YES -> jump 1 , NO -> jump 6

29.45 Are PERIMETER ZONE entries or exits by employes recorded?
YES -> jump 1 , NO -> jump 3

29.46 Are PERIMETER ZONE entries or exits by employes recorded DURING normal working hours?
YES -> jump 1 , NO -> jump 1

29.47 Are PERIMETER ZONE entries or exits by employes recorded at times OTHER THAN normal working hours?
YES -> jump 1 , NO -> jump 1

29.48 Are PERIMETER ZONE entries or exits by non-employes recorded at all times?
YES -> jump 1 , NO -> jump 2

29.49 Does the PERIMETER ZONE entry/exit record include notation for time in, time out, identification of person entering/leaving, and notation of authorization mechanism?
YES -> jump 1 , NO -> jump 1

29.50 Does the entire PERIMETER ZONE have functioning alarms or monitors (e.g., CCTV, guards, etc.) at ALL TIMES?
YES -> jump 1 , NO -> jump 9

29.51 Are there alarms, stationed guards or CCTV monitors for all PERIMETER ZONE entrances?
YES -> jump 1 , NO -> jump 1

29.52 Are there alarms, roving guards, or CCTV monitors for the PERIMETER ZONE in general?
YES -> jump 1 , NO -> jump 1

29.53 Do PERIMETER ZONE and perimeter entrance monitors and/or alarms transmit to a location where timely appropriate action will be taken?
YES -> jump 1 , NO -> jump 2

29.54 Do PERIMETER ZONE and perimeter entrance monitors and/or alarms transmit to a) a main guard station off-site, b) a local guard station on-site, c) other.
YES -> jump 1 , NO -> jump 1

29.55 Are there documented guidelines for evaluating appropriate responses to notifications from PERIMETER ZONE entrance monitors and/or alarms?
YES -> jump 1 , NO -> jump 1

29.56 Are appropriate procedures for responding to a notification from PERIMETER ZONE monitors and alarms defined and documented?
YES -> jump 1 , NO -> jump 1

29.57 Are personnel trained or drilled in how to respond to PERIMETER-ZONE monitors and alarms?
YES -> jump 1 , NO -> jump 1

29.58 Is a record from the PERIMETER ZONE and perimeter entrance monitors and alarms kept in some form available for audit?
YES -> jump 1 , NO -> jump 1

29.59 Do employes challenge persons within the PERIMETER ZONE if they are not properly identifiable?
YES -> jump 1 , NO -> jump 1

29.60 Is there a control on mechanisms (eg., badges, keys, combinations, and/or cards) used for entry to the PERIMETER ZONE?
YES -> jump 1 , NO -> jump 2

29.61 Is the control on the mechanisms used for entry to the PERIMETER ZON commensurate with the sensitivity of the assets being protected?
YES -> jump 1 , NO -> jump 1

29.62 Is the PERIMETER ZONE kept free of trash, discards, and any material that has the potential to be a weapon or a projectile?
YES -> jump 1 , NO -> jump 1

Category 30 : PERSONNEL PRIVACY

30. 1 Does the computer contain and/or process personal information about employes?
YES -> jump 1 , NO -> jump 10

30. 2 Are there control mechanisms restricting ACCESS to personal information about employes either stored in and processed by the computer system or existing in human-readable form?
YES -> jump 1 , NO -> jump 1

30. 3 Are there control mechanisms restricting MODIFICATION of personal information about employes either stored in and processed by the computer or existing in human-readable form?
YES -> jump 1 , NO -> jump 1

30. 4 Is the amount of personal information collected,stored and processed by the computer kept to the minimum necessary for the achievement of a specific purpose?
YES -> jump 1 , NO -> jump 1

30. 5 Is there provision for separating identities from personal data used for statistical purposes?
YES -> jump 1 , NO -> jump 1

30. 6 Can persons see and challenge any personal information of which he/she is the subject?
YES -> jump 1 , NO -> jump 1

30. 7 Is an audit trail available for all forms of personal information?
YES -> jump 1 , NO -> jump 1

30. 8 Is there a time limit beyond which personal information is not retained as an active file in any form?
YES -> jump 1 , NO -> jump 1

30. 9 Are there mechanisms for updating and correcting inaccuracies in personal information?
YES -> jump 1 , NO -> jump 1

30.10 Is it standard practice to encode value judgments (such as performance appraisals) made about personal information?
YES -> jump 1 , NO -> jump 1

Category 31 : STORAGE MEDIA LIBRARY

31. 1 Are magnetic tapes used at the data center?
YES -> jump 1 , NO -> jump 3

31. 2 Are all tapes (including archive tapes) tested to determine their general condition and the condition of the tape library?
YES -> jump 1 , NO -> jump 1

31. 3 Is some means used to prevent tapes from unwinding while in storage?
YES -> jump 1 , NO -> jump 1

31. 4 Are there periodic physical inventories made to assure that ALL storage media can be accounted for?
YES -> jump 1 , NO -> jump 1

31. 5 Is there a separate room or vault used as a storage media library?
YES -> jump 1 , NO -> jump 1

31. 6 Is there an accounting procedure established for media in the library?
YES -> jump 1 , NO -> jump 3

31. 7 Are all storage media removals from and returns to the library recorded?
YES -> jump 1 , NO -> jump 1

31. 8 Is a physical inventory made periodically to assure that all storage media assigned to the library's care are accounted for?
YES -> jump 1 , NO -> jump 1

31. 9 Are usage logs kept for storage media in the library?
YES -> jump 1 , NO -> jump 1

31.10 Are malfunction logs kept for storage media in the library?
YES -> jump 1 , NO -> jump 1

31.11 Is entry to the storage media library restricted to authorized personnel?
YES -> jump 1 , NO -> jump 1

31.12 Are caustic or flammable cleaning agents permitted in the storage media library?
YES -> jump 1 , NO -> jump 3

31.13 Are the caustic or flammable cleaning agents in the storage media library kept in small quantities?
YES -> jump 1 , NO -> jump 1

31.14 Are the caustic or flammable cleaning agents in the storage media library kept in approved containers?
YES -> jump 1 , NO -> jump 1

31.15 Is smoking permitted in the storage media library?
YES -> jump 1 , NO -> jump 1

31.16 Are beverages or food permitted in the storage media library?
YES -> jump 1 , NO -> jump 1

Category 32 : TERMINALS

32. 1 Are individual terminals used at the data center?
YES -> jump 1 , NO -> jump 13

32. 2 Are any authentication devices required for operating a terminal?
YES -> jump 1 , NO -> jump 2

32. 3 Indicate which devices are in use: a) keys, b) badge readers, c) magnetic card readers, d) voice print techniques, e) finger print techniques, f) other (specify).
YES -> jump 1 , NO -> jump 1

32. 4 Do the terminals have hardware-generated identifiers?
YES -> jump 1 , NO -> jump 1

32. 5 Does the operating system disconnect inactive remote terminals to preclude hidden routines that are triggered by normal operating routines ("Trojan horse" programs)?
YES -> jump 1 , NO -> jump 1

32. 6 Is the use of terminals restricted in any way?
YES -> jump 1 , NO -> jump 5

32. 7 Is each terminal limited to a specified group of users?
YES -> jump 1 , NO -> jump 1

32. 8 Are privileged functions restricted to certain terminals?
YES -> jump 1 , NO -> jump 1

32. 9 Are permitted actions at terminals defined?
YES -> jump 1 , NO -> jump 2

32.10 How are permitted actions at terminals defined: a) passwords, b) personal identifiers, c) equipment locks, d) other (specify).
YES -> jump 1 , NO -> jump 1

32.11 Is use of files from unauthorized terminals prevented?
YES -> jump 1 , NO -> jump 2

32.12 How is use of files from unauthorized terminals prevented: a) passwords, b) personal identifiers, c) equipment locks, d) other (specify).
YES -> jump 1 , NO -> jump 1

32.13 Are terminals required to be positioned so that their displays cannot be seen through doors or windows or by persons passing nearby?
YES -> jump 1 , NO -> jump 1

Category 33 : TRANSPORTATION

33. 1 Is it required to transport data, documents, or magnetic media from one site to another?
YES -> jump 1 , NO -> jump 6

33. 2 Are protective measures taken when transporting hard-copy data and documents?
YES -> jump 1 , NO -> jump 1

33. 3 Is a reputable courier service used to transport data, documents, or magnetic media from one site to another?
YES -> jump 1 , NO -> jump 1

33. 4 When transporting magnetic media, is special packaging used to protect against magnetic devices?
YES -> jump 1 , NO -> jump 1

33. 5 Are data, documents, and magnetic media insured while in transit?
YES -> jump 1 , NO -> jump 1

33. 6 Are copies made of vital and irreplaceable data, documents, and magnetic media before they are transported?
YES -> jump 1 , NO -> jump 1

Category 34 : VISITORS, VENDORS, & SERVICE PERSONNEL

34. 1 Does the data center frequently have tours or visitors from the general public?
YES -> jump 1 , NO -> jump 1

34. 2 Are all visiting personnel (vendors, consultants, contractors, service personnel, visitors, etc.) identified by some visible means such as a badge when visiting the data center?
YES -> jump 1 , NO -> jump 1

34. 3 Is photographic identification (such as a driver's license) and prior management approval required from NONEMPLOYES for entry to the data center?
YES -> jump 1 , NO -> jump 5

34. 4 Is photographic identification and prior management approval required from VENDORS for entry to the data center?
YES -> jump 1 , NO -> jump 1

34. 5 Is photographic identification and prior management approval required from SERVICE PERSONNEL for entry to the data center?
YES -> jump 1 , NO -> jump 1

34. 6 Is photographic identification and prior management approval required from CONTRACTORS for entry to the data center?
YES -> jump 1 , NO -> jump 1

34. 7 Is photographic identification and prior management approval required from OTHER VISITORS for entry to the data center?
YES -> jump 1 , NO -> jump 1

34. 8 Are background checks required for nonemployes (vendors, consultants, system/software contractors, service personnel, visitors, etc.) who require routine access to the data center?
YES -> jump 1 , NO -> jump 6

34. 9 Are background checks required for VENDORS (including vending machine attendants) who visit the data center?
YES -> jump 1 , NO -> jump 1

34.10 Are background checks required for non-employe SERVICE PERSONNEL?
YES -> jump 1 , NO -> jump 1

34.11 Are background checks required for system or software CONTRACTORS?
YES -> jump 1 , NO -> jump 1

34.12 Are background checks required for OTHER VISITORS to the facility or the data center?
YES -> jump 1 , NO -> jump 1

34.13 Are periodic follow-up background checks made on nonemployes after a period of time determined by site management?
YES -> jump 1 , NO -> jump 1

34.14 Is it policy to provide a staff escort for visitors, vendors, and service personnel in the PERIMETER ZONE?
YES -> jump 1 , NO -> jump 3

34.15 Is it policy to provide a staff escort for visitors, vendors, and service personnel in the PERIMETER ZONE DURING NORMAL business hours?
YES -> jump 1 , NO -> jump 1

34.16 Is it policy to provide a staff escort for visitors, vendors, or service personnel in the PERIMETER ZONE OUTSIDE OF NORMAL business hours?
YES -> jump 1 , NO -> jump 1

34.17 Is it policy to provide a staff escort for visitors, vendors, or service personnel in the BUILDING housing the computer equipment?
YES -> jump 1 , NO -> jump 3

34.18 Is it policy to provide a staff escort for visitors, vendors, or service personnel in the BUILDING housing the computer equipment DURING NORMAL business hours?
YES -> jump 1 , NO -> jump 1

34.19 Is it policy to provide a staff escort for visitors, vendors, or service personnel in the BUILDING housing the computer equipment OUTSIDE OF NORMAL business hours?
YES -> jump 1 , NO -> jump 1

34.20 Is it policy to provide a staff escort for visitors, vendors, or service personnel in the computer AREA?
YES -> jump 1 , NO -> jump 3

34.21 Is it policy to provide staff escort for visitors, vendors, or service personnel in the computer AREA DURING normal business hours?
YES -> jump 1 , NO -> jump 1

34.22 Is it policy to provide a staff escort for visitors, vendors, or service personnel in the computer AREA OUTSIDE OF normal business hours?
YES -> jump 1 , NO -> jump 1

34.23 Is it policy to provide a staff escort for visitors, vendors, or service personnel in the computer ROOM?
YES -> jump 1 , NO -> jump 3

34.24 Is it policy to provide a staff escort for visitors, vendors, or service personnel in the computer ROOM DURING normal business hours?
YES -> jump 1 , NO -> jump 1

34.25 Is it policy to provide a staff escort for visitors, vendors, or service personnel in the computer ROOM OUTSIDE OF normal business hours?
YES -> jump 1 , NO -> jump 1

34.26 Do operations or other employes monitor the activities of emergency, service, and other "invisible" personnel when they are servicing the computer room, area, building, or equipment?
YES -> jump 1 , NO -> jump 4

34.27 Do operations or other employes monitor the activities of emergency personnel when they are servicing the computer room, area, building, or equipment?
YES -> jump 1 , NO -> jump 1

34.28 Do operations or other employes monitor the activities of service personnel (a large part of the "invisible people") when they are servicing the computer room, area, building, or equipment?
YES -> jump 1 , NO -> jump 1

34.29 Do operations or other employes monitor the activities of other "invisible" personnel (eg, vending machine suppliers, protective force, janitors, health and safety personnel, etc.)?
YES -> jump 1 , NO -> jump 1

********** end of QUESTIONNAIRE **********

Appendix E

Bibliography

1. Abrams, M. D. et al., Tutorial on Computer Security and Integrity (IEEE Computer Society, Long Beach, CA, 1977).

2. Auerbach, Publ., Guide to Data Base Management (Auerbach Publishers, Inc., PA, 1975).

3. Barlow, R. E. and R. Proschan, Statistical Theory of Reliability and Life Testing (Holt, Rinehard, and Winston, New York, 1975).

4. Becker, R. S., The Data Processing Security Game (Pergamon Press, New York, 1977).

5. Bellman, R. E. and L. A. Zadeh, "Decision Making in a Fuzzy Environment," Management Science, Vol. 17, No. 4 (December 1970).

6. Bequai, A., Computer Crime (Lexington Books, Lexington, MA, 1978).

7. Berting, F. M., Letter to S. T. Smith, Westinghouse Hanford Company letter 8354112, November 14, 1983.

8. Bezder, J. C. and P. F. Castelaz, "Prototype Classification and Feature Selection with Fuzzy Sets," IEEE Trans. Sys.,

9. Bodily, S., "A Multiattribute Decision Analysis for the Level of Frozen Blood Utilization," IEEE Trans. Sys., Man, Cyber., Vol. SMC-7, No. 5 (May 1977).

10. Branstad, D. K. (ed.) and G. D. Cole, "Computer Science and Technology: Design Alternatives for Computer Network Security," National Bureau of Standards (U.S.) Special Publication 500-21 (January 1978).

11. Buchanan, B. G., and R. O. Duda, "Principles of Rule-Based Expert Systems," Stanford University Heuristic Programming Project Report HPP-82-14 (August 1982).

12. Buckles, B. P., and F. E. Petry, "Information - Theoretical Characterization of Fuzzy Relational Databases," IEEE Trans. Sys., Man, Cyber., Vol. SMC-13, No. 1 (January/February 1983).

13. Bushkin, A. A., "A Framework for Computer Security," System Development Corporation Report SDC-TM-WD-5733/000/01.

14. Cary, J. M., Data Security and Performance Overhead in a Distributed Architecture System (UMI Research Press, Ann Arbor, 1981).

15. Cary, J. M., Data Security and Performance Overhead in a Distributed Architecture System (UMI Research Press, Ann Arbor, MI, 1981).

16. Chang, R. L. P. and T. Pavlidis, "Fuzzy Decision Tree Algorithms," IEEE Trans. Sys, Man, Cyber., Vol SMC-7, No. 1 (January 1977).

17. Cheong, V. E., and R. A. Hirschheim, Local Area Networks: Issues, Products, and Developments, John Wiley & Sons Limited, Chichester, England (1983).

18. Computer Security Institute, Data Security Officers' Reference Manual, Course Material, 1985.

19. Computer Security Institute, Security in the Electronic Office,

Course Material, 1985.

20. Corynen, G. C., "A Methodology for Assessing the Security Risks Associated with Computer Sites and Networks. Part I: Development of a Formal Questionnaire for Collecting Security Info.," Lawrence Livermore National Lab Report UCRL-53292 Pt. 1 (June 1982).

21. Crouch, E. A. C., and R. Wilson, Risk/Benefit Analysis (Ballinger, Cambridge, MA, 1982).

22. Curry, R. E., "Worth Assessments of Approach to Landing," IEEE Trans. Sys., Man, Cyber., Vol. SMC-7, No. 5 (May 1977).

23. Data Processing Management Corporation, "A Methodology for Evaluating Alternative Technical and Information Management Approaches to Privacy Requirements," NTIS PB-254 048 (June, 1976).

24. Davies, D. W., D. L. A. Barber, W. L. Price, and C. M. Solomonides, Computer Networks and their Protocols, John Wiley & Sons Limited, Chichester, England (1981).

25. Davies, D. W., and D. L. A. Barber, Communication Networks for Computers, John Wiley & Sons Limited, Chichester, England (1973).

26. Dawes, R. M., "Predictive Models as a Guide to Preference," IEEE Trans. Sys., Man, Cyber., Vol. SMC-7, No. 5 (May 1977).

27. De, S., S.-S. Pan, and A. B. Whinston, "Natural Language Query Processing in a Temporal Database," Data and Knowledge Engineering, Vol. 1(1985) No. 1.

28. Denning, D. E. R., Cryptography and Data Security (Addison-Wesley, Reading, MA, 1983).

29. Department of Commerce, "IRS' Security Program Requires Improvements to Protect Confidentiality of Income Tax Information: Department of the Treasury," NTIS GAO PB-270 270 (July 1977).

30. Department of Defense Trusted Computer System Evaluation Criteria, CSC-STD-001-83 (August, 1983).

31. Department of Energy, "ADP Internal Control Guidelines," DOE/MA-0165 (August, 1984).

32. Department of Energy, "Computer Security Guidelines for Classified Automatic Data Processing Systems," DOE Manual 5636 (November 1979).

33. Department of Energy, "Computer Security Program for Unclassified Computer Systems," DOE Order 1360.2 (March 1979).

34. Department of Energy, "Sensitive Unclassified Computer Security Program Compliance Review Guidelines," DOE/MA-0188 (June, 1985).

35. Department of Health and Human Services, "Part 6, ADP Systems Security," HHS Transmittal 82.02 (July 1982).

36. Department of the Treasury, "IRS' Security Program Requires Improvements to Protect Confidentiality of Income Tax Information: Department of the Treasury," General Accounting Office Report NTIS PB-270270 (July 1977).

37. Dubois, D. and H. Prade, Fuzzy Sets and Systems: Theory and Applications (Academic Press, New York, 1980).

38. Edwards, W., "How to use Multiattribute Utility Measurement for Social Decisionmaking," IEEE Trans. Sys., Man, Cyber., Vol. SMC-7, No. 5 (May 1977).

39. Field, P. T., W. E. DeGrafft, and R. D. Smith, "Computer Programs for Automatically Analyzing and Drafting Fault Trees," NSRDC-4185 NSRDC-27-705 (February 1974).

40. Fishburn, P. C., "Foundations of Risk Measurement. I. Risk as Probable Loss," Management Science, Vol. 30, No. 4 (April 1984).

41. Fishburn, P. C., Decision and Value Theory (Wiley and Sons, New York, 1964).

42. Fisher, R., Information Systems Security, Prentice-Hall, Englewood Cliffs, NJ (1984).

43. Flint, D. C., The Data Ring Main: An Introduction to Local Area Networks, John Wiley & Sons Limited, Chichester, England (1983).

44. Gafni, A., and G. W. Torrance, "Risk Attitude and Time Preference in Health," Management Science, Vol. 30, No. 4 (April 1984).

45. Gardiner, P. C., "Decision Spaces," IEEE Trans. Sys., Man, Cyber., Vol. SMC-7, No. 5 (May 1977).

46. Gavison, R., "Privacy and Computerized Systems," Inf. Privacy (G.B.) Vol. 1, No. 6 (July 1979).

47. Gerberick, C., Privacy, Security, and the Information Processing Industry (ACM, Los Angeles, CA, 1977).

48. Glossbrenner, A., The Complete Handbook of Personal Computer Communications (St. Martin's Press, New York, 1983).

49. Goldstein, R. C., H. H. Seward, and R. L. Nolan, "A Methodology for Evaluating Alternative Technical and Information Management Approaches to Privacy Requirements," National Bureau of Standards Report NTIS PB-254048.

50. Gonzalez, R. C. and L. C. Howington, "Machine Recognition of Abnormal Behavior in Nuclear Reactors." IEEE Trans. Sys., Man, Cyber., Vol. SMC-7, No. 10 (October 1977).

51. Goodwin, P. G., "A Method for Evaluation of Subsystem Alternate Designs," IEEE Trans. Engr. Mgmnt., Vol. EM-19, No. 1 (February 1972).

52. Grimm, S. J., How to Write Computer Manuals for Users, Lifetime Learning Publications, Belmont, CA (1982).

53. Hammond, K. R., J. L. Mumpower, and T. H. Smith, "Linking Environmental Models with Models of Human Judgment: A Symmetrical Decision Aid," IEEE Trans. Sys., Man, Cyber., Vol. SMC-7, No. 5 (May 1977).

54. Hartley, R. T., "How Expert Should an Expert System Be?" Proc. 7th Joint Conf. on Artificial Intelligence, Vancouver, BC, Canada (August 1981).

55. Hayes-Roth, F., D. A. Waterman, and D. B. Lenat (eds.), Building Expert Systems, Addison-Wesley, Reading, MA (1983).

56. Heinrich, F., "The Network Security Center: A System Level Approach to Computer Network Security," National Bureau of Standards (U.S.) Special Publication 500-21, Vol. 2 (January 1978).

57. Hoffman, L. J., Modern Methods for Computer Security and Privacy (Prentice-Hall, Inc., Englewood Cliffs, NJ, 1977).

58. Hoffman, L. J., Security and Privacy in Computer Systems (Melville Publishing Co., Los Angeles, 1973).

59. Howard, R. A., "On Fates Comparable to Death," Management Science, Vol. 30, No. 4 (April 1984).

60. Hsiao, D. K., D. S. Keer, and S. E. Madnick, Computer Security, Academic Press, New York (1979).

61. Jain, R., "A Procedure for Multiple-Aspect Decision-Making Using Fuzzy Sets," Int. J. Systems Sci., Vol. 8, No. 1, pp. 1-7 (January 1977).

62. Jaske, M. R., "Interfacing Large Interactive Systems Models and the User," IEEE Trans. Sys., Man, Cyber., Vol. SMC-7, No. 5 (May 1977).

63. Johnson, E. M., and G. P. Huber, "The Technology of Utility Assessment," IEEE Trans. Sys., Man, Cyber., Vol. SMC-7, No. 5 (May 1977).

64. Kaplan, S., and B. J. Garrick, "On the Use of Bayesian Reasoning in Safety and Reliability Decisions - Three Examples," Nuclear Technology, Vol. 44 (July 1979).

65. Kilgore, G. A., "Probabilistic Measures of Compromise," USAF Report ESD-TR-76-160 (January 1976).

66. Klee, A. J., "The Role of Decision Models in the Evaluation of Competing Environmental Health Alternatives," Management Science, Vol. 18, No. 2 (October 1971).

67. Kleinman, D. L., and R. E. Curry, "Some New Control Theoretic Models for Human Operator Display Monitoring," IEEE Trans. Sys., Man, Cyber., Vol. SMC-7, No. 11 (November 1977).

68. Konheim, A. G., Cryptography: A Primer (Wiley and Sons, New York, 1981).

69. Krauss, L. I., SAFE: Security Audit and Field Evaluation for Computer Facilities and Information Systems (AMACOM, New York, 1980).

70. Krauss, L. I., and A. MacGahan, Computer Fraud and Countermeasures (Prentice-Hall, Inc., Englewood Cliffs, NJ, 1979).

71. Kunreuther, H., J. Linnerooth, and J. W. Vaupel, "A Decision-Process Perspective on Risk and Policy Analysis," Management Science, Vol. 30, No. 4 (April 1984).

72. Kusserow, R. P., "Computer-Related Fraud and Abuse in Government Agencies," U.S. Department HHS Report, June, 1983.

73. Kvalseta, T. O., "A Decision-Theoretic Model of the Sampling Behavior of the Human Process Monitor," IEEE Trans. Sys., Man,

Cyber., Vol. SMC-7, No. 11 (November 1977).

74. Lambert, H. E., "Fault Trees for Decision Making in Systems Analysis," UCRL-51829 (October, 1975).

75. Leal, A., and J. Pearl, "An Interactive Program for Conversational Elicitation of Decision Structures," IEEE Trans. Sys., Man, Cyber., Vol. SMC-7, No. 5 (May 1977).

76. Main, G. C., "RL Computer Protection Program - Application System Risk Analysis Methodology," BCSR-ADS-1235, September, 1981.

77. Main, G. C., "RL Computer Protection Program - Application System Sensitivity Determination," BCSR-ADS-0234A, August, 1982.

78. Main, G. C., "Software/Applications Risk Analysis," Sixth DOE Computer Security Conference, Lakewood, CO, July 26-28, 1983.

79. Martin, J., Security, Accuracy, and Privacy in Computer Systems (Prentice-Hall, Inc., Englewood Cliffs, NJ, 1973).

80. Martin-Marietta Energy Systems, ADP Protection Handbook (March, 1984).

81. McCormick, N. J., Reliability and Risk Analysis (Academic Press, New York, 1981).

82. Mesarovic, M. D., D. Macko, and Y. Takahara, Theory of Hierarchical Multilevel Systems (Academic Press, New York, 1980).

83. Meyer, C. H., and S. M. Matyas, Cryptography: A New Dimension in Computer Data Security, John Wiley & Sons Limited, Chichester, England (1982).

84. Milton, R. C., Rank Order Probabilities (Wiley and Sons, New York, 1970).

85. Mullen, R. K., "Sabotage Threats to Energy Assets," International Association of Chiefs of Police Report, Gaithersburg, MD, 1983.

86. Mullen, R. K., "Sabotage Threats to Energy Assets," Int'l. Ass'n. of Chiefs of Police Meeting (1983).

87. Mullen, S. A., J. J. Davidson, and H. B. Jones, Jr., "Potential Threat to Licensed Nuclear Activities from Insiders (Insider Study)," U. S. Nuclear Regulatory Commission Report NUREG-0703 (July 1980).

88. National Bureau of Standards, "An Analysis of Computer Security Safeguards for Detecting and Preventing Intentional Computer Misuse," NBS Special Publication 500-25 (1978).

89. National Bureau of Standards, "Guideline on User Authentication Techniques for Computer Network Access Control," Federal Information Processing Standard Publication FIPS-PUB-83 (September 1980).

90. National Bureau of Standards, "Guidelines for Automatic Data Processing, Physical Security, and Risk Management," Federal Information Processing Standards Publication FIPS-PUB-31 (June 1974).

91. National Bureau of Standards, "Guidelines for Computer Security Certification and Accreditation," Federal Information Processing Standards Publication FIPS-PUB-102 (September 1983).

92. National Bureau of Standards, "Guidelines on Electrical Power for ADP Installations," Federal Information Processing Standards Publication FIPS-PUB-94 (September 1983).

93. National Fire Prevention and Control Administration, "Standard Practice for the Fire Protection of Essential Electronic Equipment Operations," NTIS PB-287 292 (August, 1978).

94. Naylor, C., Build Your Own Expert System, John Wiley & Sons,

New York (1985).

95. Negoita, C. V. (1985). Expert Systems and Fuzzy Systems. The Benjamin/Cummings Publishing Company, Inc., Menlo Park, CA.

96. Neilsen, N. R., D. H. Brandin, J. D. Madden, B. Ruder, G. F. Wallace, "Computer System Integrity Safeguards: System Integrity Maintenance," SRI Project No. 4059 Final Report (October 1976).

97. Neilson, N. R., B. Ruder, J. D. Madden, and P. J. Wong, "Computer System Integrity: A Relative - Impact Measure of Vulnerability," SRI International Report SRI Project 4059 (June 1978).

98. Nilsson, N. R., Principles of Artificial Intelligence (Tioga Publishing Co., Palo Alto, 1980).

99. Okrent, D., "A General Evaluation Approach to Risk-Benefit for Large Technological Systems and Its Application to Nuclear Power," UCLA-ENG-7777 (December, 1977).

100. Ombudsman Committee on Privacy, "Privacy, Security, and the Information Processing Industry," sponsored by The Association for Computing Machinery, Los Angeles, 1976.

101. Pacific Northwest Laboratory ADP Risk Assessment Document, "Computer Hardware," Batelle Form A-1004-125, March, 1983.

102. Pacific Northwest Laboratory ADP Risk Assessment Document, "Software Applications," Batelle Form A-1004-124, March, 1983.

103. Parker, Donn B., Crime by Computer (Scribner's Sons, New York, 1976).

104. Parker, Donn B., Fighting Computer Crime (Scribner's Sons, New York, 1983).

105. Parsaye, K., "Database Management, Knowledge Base Management, and Expert System Development in PROLOG," ACM 0-89791-105-

9/83/005/0159 (1983).

106. Pearl, J., Heuristics: Intelligent Search Strategies for Computer Problem Solving, Addison-Wesley, New York (1984).

107. Pearl, Judea, "A Framework for Processing Value Judgments," IEEE Trans. Sys., Man, Cyber., Vol. SMC-7, No. 5 (May 1977).

108. Perry, W. E., Computer Control and Security (John Wiley and Sons, New York, 1981).

109. Prague, C. N., and J. E. Hammit, Programming with dBASE II (TAB Books, Blue Ridge Summit, PA, 1984).

110. Raiffa, H., Decision Analysis (Addison-Wesley, Reading, MA, 1970).

111. Raphael, B., The Thinking Computer: Mind Inside Matter (W H Freeman and Co, San Francisco, 1976).

112. Ratliff, W., dBASE II: Assembly Language Relational Database Management System (Ashton-Tate, Culver City, CA, 1982).

113. Reed, S. K., "Automatic Data Processing Risk Assessment," National Bureau of Standards Report NTIS PB-265950 (March 1977).

114. Reed, S. K., "Guideline for Automatic Data Processing Risk Analysis," FIPS-PUB-65, National Bureau of Standards (August 1979).

115. Rouse, W. B., and R. M. Hunt, "A Fuzzy Rule-Based Model of Human Problem-Solving in Fault Diagnosis Tasks," Proc. Eighth Triennial World Congress of the International Federation of Automatic Control, Kyoto, Japan (August 1981).

116. Rowe, W. D., An Anatomy of Risk (Wiley and Sons, New York, 1977).

117. Ruder, B., J. D. Madden, and R. P. Blanc, "Computer Science and Technology: An Analysis of Computer Security Safeguards for Detecting and Preventing Intentional Computer Misuse," Nat. Bureau of Stand. (U.S.) Special Publication 500-25 (January 1978).

118. Rullo, T. A., Advances in Computer Security Management (Heyden & Son, Inc., Philadelphia, 1980).

119. Rullo, T. A., Advances in Computer Security Management, Vol. 1 (Heyden, Philadelphia, 1980).

120. Ruthberg, Z. G., and R. G. McKenzie (eds.), "Audit and Evaluation of Computer Security," National Bureau of Standards Special Publication 500-19 (October 1977).

121. Sarin, R. K., "A Social Decision Analysis of the Earthquake Safety Problem: The Case of Existing Los Angeles Buildings," Risk Analysis, Vol. 3, No. 1 (January 1983).

122. Schacht, J. M., S. M. Goheen, and R. D. Rhode, "User Requirements for Computer Security," USAF System Command Report ESD-TR-79-127 (August 1979).

123. Schank, R. C., with P. G. Childers, The Cognitive Computer (Addison-Wesley, New York, 1984).

124. Schlaifer, R., Introduction to Statistics for Business Decisions (McGraw-Hill, 1961).

125. Schlaifer, R., Probability and Statistics for Business Decisions (McGraw-Hill, New York, 1959).

126. Schmucker, K. J., Fuzzy Sets, Natural Language Computations, and Risk Analysis (Computer Science Press, Rockville, MD, 1984).

127. Schmucker, K. J., Fuzzy Sets, Natural Language, and Risk Analysis: A Tutorial (George Washington University,

Washington, DC, October 1981).

128. Schoemaker, P. J. H., and C. Waid, "An Experimental Comparison of Different Approaches to Determining Weights in Additive Utility Models," Management Science, Vol. 28, No. 2 (February 1982).

129. Sheridan, T. B., and A. Sickerman, "Estimation of a Group's Multiattribute Utility Function in Real Time by Anonymous Voting," IEEE Trans. Sys., Man, Cyber., Vol. SMC-7, No. 5 (May 1977).

130. Slovic, P., S. Lichtenstein, and B. Fischoff, "Modeling the Societal Impact of Total Accidents," Management Science, Vol. 30, No. 4 (April 1984).

131. Spetzler, C. S., and C. A. S. Stael von Holstein, "Probability Encoding in Decision Analysis," Management Science, Vol. 22, No. 3 (November 1975).

132. Squires, T., Computer Security - the Personnel Aspect (NCC Publications, Manchester, England, 1980).

133. Stallings, W., "Fuzzy Set Theory Versus Bayesian Statistics," IEEE Trans. Sys., Man, Cyber., Vol. SMC-7, No. 3 (March 1977).

134. Starr, C., and C. Whipple, "A Perspective on Health and Safety Risk Analysis," Management Science, Vol. 30, No. 4 (April 1984).

135. Steinauer, D. D., "Security of Personal Computers: A Management Guide," National Bureau of Standards Special Pub. 500-120, January, 1985.

136. Stimson, D. H., "Utility Measurement in Public Health Decision Making," Management Science Vol. 16, No. 2 (October 1969).

137. Stroik, J. (ed), "Building Security," Symposium sponsored by ASTM Committee F-12 on Security Systems and Equipment,

Gaithersburg, 1979.

138. Sudman, S. and N. M. Bradburn, Asking Questions: A Practical Guide to Questionnaire Design (Jassey-Bass, Inc, San Francisco, 1982).

139. System Development Corporation, "Risk Assessment Methodology," Defense Logistics Agency Report TM-WD-7999/001/03 (July 1979).

140. Systems Development Corporation, "Risk Assessment Methodology," NTIS TM-WD-7999/001/03 (July, 1979).

141. Talbot, J. R., Management Guide to Computer Security (John Wiley and Sons, New York, 1981).

142. Thomas, J. M., "Decision Methods in Risk Analysis," Nuclear Engineering and Design 71 (August 1982).

143. Troy, E. F., "Thwarting the Hackers," Datamation, July 1, 1984, pp. 117-127.

144. Turn, R. (ed.), Advances in Computer Security (Artech House, Inc., MA, 1981).

145. USA. ADP System Security Enhancement Program, "Lessons Learned FY82," ADP Systems Security Div., 902d Military Intelligence Gr., Fort George G. Meade, MD (January 1983).

146. Van Tassel, D., Computer Security Management (Prentice-Hall Inc., Englewood Cliffs, NJ, 1972).

147. Webster, E. (ed.), Data Communications and Business Systems (International Business Forms Industries, Arlington, VA, 1971).

148. Weintraub, A. A., and T. P. O'Connor, "Standard for Fire Protection of AEC Electronic Computer/Data Processing Systems," USAEC Report Wash 1245-1 (July 1973).

149. Weisbrod, R. L., K. B. Davis, and A. Freedy, "Adaptive Utility Assessment in Dynamic Decision Processes: An Experimental Evaluation of Decision Aiding," IEEE Trans. Sys., Man, Cyber., Vol. SMC-7, No. 5 (May 1977).

150. West, E. et al., "RP-1: Standard Practice for the Fire Protection of Essential Electronic Equipment Operations," National Fire Prevention and Control Administration Report PB287292 (August 1978).

151. White, D. R. J., D. L. Scott, and R. N. Schulz, "POED - A Method of Evaluating System Performance," IEEE Trans. Engr. Mgmnt., Vol. EM-10, No. 12 (December 1963).

152. Whitty, W. J., "An Evaluation Procedure for Radioactive Waste Treatment," Los Alamos National Laboratory Report LA-8052-MS (November 1979).

153. Winston, P. H., Artificial Intelligence (2nd Ed.), Addison-Wesley, New York (1984).

154. Wong, K. K., Computer Security Risk Analysis and Control: A Guide for the DP Manager (NCC/Hayden, Manchester, England, 1977).

155. Zadeh, L. A., "PRUF: A Meaning Representation for Natural Language," Memo ERL M77/61, University of California at Berkeley (1977).

156. Zadeh, L. A., "The Role of Fuzzy Logic in the Management of Uncertainty in Expert Systems," Memo UCB/ERL M83/41, University of California at Berkeley (July 1983).

157. Zadeh, L. A., K.-S. Fu, K. Tanaka, and M. Shimura, Fuzzy Sets and Their Application to Cognitive and Decision Processes (Academic Press, New York, 1975).

Appendix F

User's Support Information

Telephone support is provided for all aspects of LAVA/CS Version 1.01. If a problem arises during your use of the LAVA program, we encourage you to contact the LAVA/CS Development Team in care of the Department of Energy Center for Computer Security:

Commercial	(505) 667-0444
FTS	843-0444

For assistance by mail, please send your requests to

LAVA/CS Development Team
DOE Center for Computer Security
Los Alamos National Laboratory
P.O. Box 1663 MS E541
Los Alamos, NM 87545

We encourage you to read the section in the manual dealing with the part of LAVA/CS you are experiencing problems with before contacting us. In the event that the manual does not provide the necessary information to remedy your situation, an accurate trace-back of the events leading to the problem is vital. To enable us to better assist you with implementation problems, please obtain a hardcopy of the screen where the error occurred and be prepared to provide us with the following information:

Hardware Configuration

1. What make and model of compu r are you using?
2. How much physical memory (F .M) does your computer have?
3. What disk-drive configuration do you have?
4. Does your computer support graphics? If so, what kind?

Software Configuration

1. What version of LAVA/CS are you using?
2. What version of DOS are you using?
3. Are you using any graphics software?

A limited number of software packages are available through the DOE Center for Computer Security for DOE site and DOE contractors. All other government agencies should contact

National Energy Software Center
Argonne National Laboratory
9700 S. Cass Avenue
Argonne, Illinois 603439

Commercial (312) 972-7250
FTS 972-7250

to obtain copies of the LAVA/CS software package. There will be a minimal fee to cover duplication costs for each software package obtained through the National Energy Software Center.

Your suggestions on improvements to the LAVA/CS software and this user's manual are solicited. Please mail your suggestions to the LAVA Development Team at the DOE Center for Computer Security.